FISC Security Reference Response Guide

Facility	
List of Measures in the FISC Security Guidelines	
Item No.	Google Response
F1	Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001:2013, Annex A.11). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google designs the components of our platform to be highly redundant. This redundancy applies to our server design, how we store data, network and internet connectivity, and the software services themselves. This “redundancy of everything” includes the handling of errors by design and creates a solution that is not dependant on a single server, data center, or network connection. Google’s data centers are geographically distributed to minimize the effects of regional disruptions such as natural disasters and local outages. In the event of hardware, software, or network failure, data is automatically shifted from one facility to another so that Google Cloud and G Suite customers can continue working in most cases without interruption. Google’s highly redundant infrastructure also helps protect our customers from data loss. For Google Cloud Products (G Suite and Google Cloud Platform), our Recovery Point Objective (RPO) target is zero, and our recovery time objective (RTO) design target is also zero. We aim to achieve these targets through live or synchronous replication: actions you take in Cloud products are simultaneously replicated in two data centers at once, so that if one data center fails, we transfer your data over to the other one that's also been reflecting your actions. Google adheres to all building and facility requirements in the region where its data centers are located.
F2	Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001:2013, Annex A.11). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google designs the components of our platform to be highly redundant. This redundancy applies to our server design, how we store data, network and internet connectivity, and the software services themselves. This “redundancy of everything” includes the handling of errors by design and creates a solution that is not dependant on a single server, data center, or network connection. Google’s data centers are geographically distributed to minimize the effects of regional disruptions such as natural disasters and local outages. In the event of hardware, software, or network failure, data is automatically shifted from one facility to another so that Google Cloud and G Suite customers can continue working in most cases without interruption. Google’s highly redundant infrastructure also helps protect our customers from data loss. For Google Cloud Products (G Suite and Google Cloud Platform), our Recovery Point Objective (RPO) target is zero, and our recovery time objective (RTO) design target is also zero. We aim to achieve these targets through live or synchronous replication: actions you take in Cloud products are simultaneously replicated in two data centers at once, so that if one data center fails, we transfer your data over to the other one that's also been reflecting your actions. Google adheres to all building and facility requirements in the region where its data centers are located.
F3	Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001:2013, Annex A.11). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Environmental health and safety controls are implemented at all Google Data Centers. All sites provide robust fire protection, detection and prevention. Fire detection and suppression equipment helps prevent damage to hardware. Heat, fire, and smoke detectors trigger aud ble and visible alarms in the affected zone, at security operations consoles, and at remote monitoring desks. Google adheres to all building requirements in the region where its data centers are located. More details can be found in Google's Security Whitepaper: https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers Google adheres to all building and facility requirements in the region where its data centers are located.
F4	Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001:2013, Annex A.11). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Environmental health and safety controls are implemented at all Google Data Centers. All sites provide robust fire protection, detection and prevention. Fire detection and suppression equipment helps prevent damage to hardware. Heat, fire, and smoke detectors trigger aud ble and visible alarms in the affected zone, at security operations consoles, and at remote monitoring desks. Google adheres to all building requirements in the region where its data centers are located. More details can be found in Google's Security Whitepaper: https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers Google adheres to all building and facility requirements in the region where its data centers are located.
F5	Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001:2013, Annex A.11). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google’s focus on security and protection of data is among our primary design criteria. Google data center physical security features a layered security model, including safeguards l ke custom-designed electronic access cards, alarms, vehicle access barriers, perimeter fencing, metal detectors, biometrics, and the data center floor features laser beam intrusion detection. Our data centers are monitored 24/7 by high-resolution interior and exterior cameras that can detect and track intruders. Access logs, activity records, and camera footage are available in case an incident occurs. Data centers are also routinely patrolled by experienced security guards who have undergone rigorous background checks and training. To learn more about our Data Center Processes, please see our Security Whitepaper and Data Center Introduction videos: Google Security Whitepaper: https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers Data Center Introduction Video: https://www.youtube.com/watch?v=XZmGGAbHqa0 Google adheres to all building and facility requirements in the region where its data centers are located.
F6	Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001:2013, Annex A.11). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google’s focus on security and protection of data is among our primary design criteria. Google data center physical security features a layered security model, including safeguards l ke custom-designed electronic access cards, alarms, vehicle access barriers, perimeter fencing, metal detectors, biometrics, and the data center floor features laser beam intrusion detection. Our data centers are monitored 24/7 by high-resolution interior and exterior cameras that can detect and track intruders. Access logs, activity records, and camera footage are available in case an incident occurs. Data centers are also routinely patrolled by experienced security guards who have undergone rigorous background checks and training. To learn more about our Data Center Processes, please see our Security Whitepaper and Data Center Introduction videos: Google Security Whitepaper: https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers Data Center Introduction Video: https://www.youtube.com/watch?v=XZmGGAbHqa0 Google adheres to all building and facility requirements in the region where its data centers are located.
F7	Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001:2013, Annex A.11). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. To learn more about our Data Center Processes, please see our Security Whitepaper and Data Center Introduction videos: Google Security Whitepaper: https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers Data Center Introduction Video: https://www.youtube.com/watch?v=XZmGGAbHqa0" Google adheres to all building and facility requirements in the region where its data centers are located.
F8	Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001:2013, Annex A.11). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Physical access to secured areas (such as the data server floor) is only possible via a security corridor. Google implements multi-factor access control using security badges and biometrics. Only approved employees with specific roles may enter secured areas, and all access to those area is monitored, logged and periodically approved for appropriateness. Google adheres to all building and facility requirements in the region where its data centers are located.

F9	Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001:2013, Annex A.11). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. To keep things running 24/7 and ensure uninterrupted services Google’s data centers feature redundant power systems and environmental controls. Every critical component has a primary and alternate power source, each with equal power. Diesel engine backup generators can provide enough emergency electrical power to run each data center at full capacity. Cooling systems maintain a constant operating temperature for servers and other hardware, reducing the risk of service outages. Fire detection and suppression equipment helps prevent damage to hardware. Heat, fire, and smoke detectors trigger audible and vis ble alarms in the affected zone, at security operations consoles, and at remote monitoring desks. Google adheres to all building and facility requirements in the region where its data centers are located.
F10	Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001:2013, Annex A.11). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Environmental health and safety controls are implemented at all Google Data Centers. All sites provide robust fire protection, detection and prevention. Fire detection and suppression equipment helps prevent damage to hardware. Heat, fire, and smoke detectors trigger aud ble and visible alarms in the affected zone, at security operations consoles, and at remote monitoring desks. Google adheres to all building requirements in the region where its data centers are located. More details can be found in Google's Security Whitepaper: https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers Google adheres to all building and facility requirements in the region where its data centers are located.
F11	Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001:2013, Annex A.11). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Environmental health and safety controls are implemented at all Google Data Centers. All sites provide robust fire protection, detection and prevention. Fire detection and suppression equipment helps prevent damage to hardware. Heat, fire, and smoke detectors trigger aud ble and visible alarms in the affected zone, at security operations consoles, and at remote monitoring desks. Google adheres to all building requirements in the region where its data centers are located. More details can be found in Google's Security Whitepaper: https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers Google adheres to all building and facility requirements in the region where its data centers are located.
F12	Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001:2013, Annex A.11). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. To keep things running 24/7 and ensure uninterrupted services Google’s data centers feature redundant power systems and environmental controls. Every critical component has a primary and alternate power source, each with equal power. Diesel engine backup generators can provide enough emergency electrical power to run each data center at full capacity. Cooling systems maintain a constant operating temperature for servers and other hardware, reducing the risk of service outages. Fire detection and suppression equipment helps prevent damage to hardware. Heat, fire, and smoke detectors trigger audible and vis ble alarms in the affected zone, at security operations consoles, and at remote monitoring desks. Google adheres to all building and facility requirements in the region where its data centers are located.
F13	Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001:2013, Annex A.11). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google’s focus on security and protection of data is among our primary design criteria. Google data center physical security features a layered security model, including safeguards l ke custom-designed electronic access cards, alarms, vehicle access barriers, perimeter fencing, metal detectors, biometrics, and the data center floor features laser beam intrusion detection. Our data centers are monitored 24/7 by high-resolution interior and exterior cameras that can detect and track intruders. Access logs, activity records, and camera footage are available in case an incident occurs. Data centers are also routinely patrolled by experienced security guards who have undergone rigorous background checks and training. Google adheres to all building and facility requirements in the region where its data centers are located.
F14	Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001:2013, Annex A.11). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Environmental health and safety controls are implemented at all Google Data Centers. All sites provide robust fire protection, detection and prevention. Fire detection and suppression equipment helps prevent damage to hardware. Heat, fire, and smoke detectors trigger aud ble and visible alarms in the affected zone, at security operations consoles, and at remote monitoring desks. Google adheres to all building requirements in the region where its data centers are located. More details can be found in Google's Security Whitepaper: https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers Google adheres to all building and facility requirements in the region where its data centers are located.
F15	Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001:2013, Annex A.11). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google’s focus on security and protection of data is among our primary design criteria. Google data center physical security features a layered security model, including safeguards l ke custom-designed electronic access cards, alarms, vehicle access barriers, perimeter fencing, metal detectors, biometrics, and the data center floor features laser beam intrusion detection. Our data centers are monitored 24/7 by high-resolution interior and exterior cameras that can detect and track intruders. Access logs, activity records, and camera footage are available in case an incident occurs. Data centers are also routinely patrolled by experienced security guards who have undergone rigorous background checks and training. Google adheres to all building and facility requirements in the region where its data centers are located.
F16	Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001:2013, Annex A.11). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Physical access to secured areas (such as the data server floor) is only possible via a security corridor. Google implements multi-factor access control using security badges and biometrics. Only approved employees with specific roles may enter secured areas, and all access to those area is monitored and logged. Google’s focus on security and protection of data is among our primary design criteria. Google data center physical security features a layered security model, including safeguards l ke custom-designed electronic access cards, alarms, vehicle access barriers, perimeter fencing, metal detectors, biometrics, and the data center floor features laser beam intrusion detection. Our data centers are monitored 24/7 by high-resolution interior and exterior cameras that can detect and track intruders. Access logs, activity records, and camera footage are available in case an incident occurs. Data centers are also routinely patrolled by experienced security guards who have undergone rigorous background checks and training. Google adheres to all building and facility requirements in the region where its data centers are located.
F17	Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001:2013, Annex A.11). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Environmental health and safety controls are implemented at all Google Data Centers. Employee safety is the most important of all consideration and appropriate signs are posted and training conducted to ensure all staff can safely evacuate in case of an emergency. All sites provide robust fire protection, detection and prevention. Fire detection and suppression equipment helps prevent damage to hardware. Heat, fire, and smoke detectors trigger aud ble and visible alarms in the affected zone, at security operations consoles, and at remote monitoring desks. More details can be found in Google's Security Whitepaper: https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers Google adheres to all building and facility requirements in the region where its data centers are located.

F18	Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001:2013, Annex A.11). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Environmental health and safety controls are implemented at all Google Data Centers. All sites provide robust detection of environmental elements, including heat, fire, smoke and water detection. All sites provide robust fire protection, detection and prevention. Fire detection and suppression equipment helps prevent damage to hardware. Heat, fire, smoke, and water detectors trigger audible and visible alarms in the affected zone, at security operations consoles, and at remote monitoring desks. Google adheres to all building requirements in the region where its data centers are located. More details can be found in Google's Security Whitepaper: https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers Google adheres to all building and facility requirements in the region where its data centers are located.
F19	Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001:2013, Annex A.11). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google's focus on security and protection of data is among our primary design criteria. Google data center physical security features a layered security model, including safeguards like custom-designed electronic access cards, alarms, vehicle access barriers, perimeter fencing, metal detectors, biometrics, and the data center floor features laser beam intrusion detection. Our data centers are monitored 24/7 by high-resolution interior and exterior cameras that can detect and track intruders. Access logs, activity records, and camera footage are available in case an incident occurs. Data centers are also routinely patrolled by experienced security guards who have undergone rigorous background checks and training. Physical access to secured areas (such as the data server floor) is only possible via a security corridor. Google implements multi-factor access control using security badges and biometrics. Only approved employees with specific roles may enter secured areas, and all access to those area is monitored and logged. Google adheres to all building and facility requirements in the region where its data centers are located.
F20	Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001:2013, Annex A.11). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Environmental health and safety controls are implemented at all Google Data Centers. All sites provide robust fire protection, detection and prevention. Fire detection and suppression equipment helps prevent damage to hardware. Heat, fire, and smoke detectors trigger audible and visible alarms in the affected zone, at security operations consoles, and at remote monitoring desks. Google adheres to all building requirements in the region where its data centers are located. More details can be found in Google's Security Whitepaper: https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers Google adheres to all building and facility requirements in the region where its data centers are located.
F21	Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001:2013, Annex A.11). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. To keep things running 24/7 and ensure uninterrupted services Google's data centers feature redundant power systems and environmental controls. Every critical component has a primary and alternate power source, each with equal power. Diesel engine backup generators can provide enough emergency electrical power to run each data center at full capacity. Cooling systems maintain a constant operating temperature for servers and other hardware, reducing the risk of service outages. Fire detection and suppression equipment helps prevent damage to hardware. Heat, fire, and smoke detectors trigger audible and visible alarms in the affected zone, at security operations consoles, and at remote monitoring desks. Google adheres to all building and facility requirements in the region where its data centers are located and maintains facilities that comply with best practices to minimize damage due to natural disasters.
F22	Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001:2013, Annex A.11). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. To keep things running 24/7 and ensure uninterrupted services Google's data centers feature redundant power systems and environmental controls. Every critical component has a primary and alternate power source, each with equal power. Diesel engine backup generators can provide enough emergency electrical power to run each data center at full capacity. Cooling systems maintain a constant operating temperature for servers and other hardware, reducing the risk of service outages. Fire detection and suppression equipment helps prevent damage to hardware. Heat, fire, and smoke detectors trigger audible and visible alarms in the affected zone, at security operations consoles, and at remote monitoring desks. Google adheres to all building and facility requirements in the region where its data centers are located and maintains facilities that comply with best practices to minimize damage due to natural disasters.
F23	Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001:2013, Annex A.11). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Physical access to secured areas (such as the data server floor) is only possible via a security corridor. Google implements multi-factor access control using security badges and biometrics. Only approved employees with specific roles may enter secured areas, and all access to those area is monitored, logged and periodically approved for appropriateness. Google adheres to all building and facility requirements in the region where its data centers are located.
F24	Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001:2013, Annex A.11). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google's focus on security and protection of data is among our primary design criteria. Google data center physical security features a layered security model, including safeguards like custom-designed electronic access cards, alarms, vehicle access barriers, perimeter fencing, metal detectors, biometrics, and the data center floor features laser beam intrusion detection. Our data centers are monitored 24/7 by high-resolution interior and exterior cameras that can detect and track intruders. Access logs, activity records, and camera footage are available in case an incident occurs. Data centers are also routinely patrolled by experienced security guards who have undergone rigorous background checks and training. To learn more about our Data Center Processes, please see our Security Whitepaper and Data Center Introduction videos: Google Security Whitepaper: https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers Data Center Introduction Video: https://www.youtube.com/watch?v=XZmGGAbHqa0 Google adheres to all building and facility requirements in the region where its data centers are located.
F25	Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001:2013, Annex A.11). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Environmental health and safety controls are implemented at all Google Data Centers. Employee safety is the most important of all consideration and appropriate signs are posted and training conducted to ensure all staff can safely evacuate in case of an emergency. All sites provide robust fire protection, detection and prevention. Fire detection and suppression equipment helps prevent damage to hardware. Heat, fire, and smoke detectors trigger audible and visible alarms in the affected zone, at security operations consoles, and at remote monitoring desks. Google adheres to all building requirements in the region where its data centers are located. More details can be found in Google's Security Whitepaper: https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers Google adheres to all building and facility requirements in the region where its data centers are located.
F26	Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001:2013, Annex A.11). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google designs the components of our platform to be highly redundant. This redundancy applies to our server design, how we store data, network and internet connectivity, and the software services themselves. This "redundancy of everything" includes the handling of errors by design and creates a solution that is not dependant on a single server, data center, or network connection. Google's data centers are geographically distributed to minimize the effects of regional disruptions such as natural disasters and local outages. In the event of hardware, software, or network failure, data is automatically shifted from one facility to another so that Google Cloud and G Suite customers can continue working in most cases without interruption. Google's highly redundant infrastructure also helps protect our customers from data loss. For Google Cloud Products (G Suite and Google Cloud Platform), our Recovery Point Objective (RPO) target is zero, and our recovery time objective (RTO) design target is also zero. We aim to achieve these targets through live or synchronous replication: actions you take in Cloud products are simultaneously replicated in two data centers at once, so that if one data center fails, we transfer your data over to the other one that's also been reflecting your actions. Google adheres to all building and facility requirements in the region where its data centers are located.

F27	Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001:2013, Annex A.11). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Environmental health and safety controls are implemented at all Google Data Centers. Employee safety is the most important of all consideration and appropriate signs are posted and training conducted to ensure all staff can safely evacuate in case of an emergency. All sites provide robust fire protection, detection and prevention. Fire detection and suppression equipment helps prevent damage to hardware. Heat, fire, and smoke detectors trigger audible and visible alarms in the affected zone, at security operations consoles, and at remote monitoring desks. More details can be found in Google's Security Whitepaper: https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers Google adheres to all building and facility requirements in the region where its data centers are located.
F28	Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001:2013, Annex A.11). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google's focus on security and protection of data is among our primary design criteria. Google data center physical security features a layered security model, including safeguards like custom-designed electronic access cards, alarms, vehicle access barriers, perimeter fencing, metal detectors, biometrics, and the data center floor features laser beam intrusion detection. Our data centers are monitored 24/7 by high-resolution interior and exterior cameras that can detect and track intruders. Access logs, activity records, and camera footage are available in case an incident occurs. Data centers are also routinely patrolled by experienced security guards who have undergone rigorous background checks and training. To learn more about our Data Center Processes, please see our Security Whitepaper and Data Center Introduction videos: Google Security Whitepaper: https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers Data Center Introduction Video: https://www.youtube.com/watch?v=XZmGGAbHqa0 Google adheres to all building and facility requirements in the region where its data centers are located.
F29	Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001:2013, Annex A.11). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Environmental health and safety controls are implemented at all Google Data Centers. All sites provide robust detection of environmental elements, including heat, fire, smoke and water detection. All sites provide robust fire protection, detection and prevention. Fire detection and suppression equipment helps prevent damage to hardware. Heat, fire, smoke, and water detectors trigger audible and visible alarms in the affected zone, at security operations consoles, and at remote monitoring desks. Google adheres to all building requirements in the region where its data centers are located. More details can be found in Google's Security Whitepaper: https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers Google adheres to all building and facility requirements in the region where its data centers are located.
F30	Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001:2013, Annex A.11). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Environmental health and safety controls are implemented at all Google Data Centers. Employee safety is the most important of all consideration and appropriate signs are posted and training conducted to ensure all staff can safely evacuate in case of an emergency. All sites provide robust fire protection, detection and prevention. Fire detection and suppression equipment helps prevent damage to hardware. Heat, fire, and smoke detectors trigger audible and visible alarms in the affected zone, at security operations consoles, and at remote monitoring desks. More details can be found in Google's Security Whitepaper: https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers Google adheres to all building and facility requirements in the region where its data centers are located.
F31	Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001:2013, Annex A.11). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Environment health and safety controls are implemented at all Google Data Centers. All sites provide robust fire protection, detection and prevention. Fire detection and suppression equipment helps prevent damage to hardware. Heat, fire, and smoke detectors trigger audible and visible alarms in the affected zone, at security operations consoles, and at remote monitoring desks. Google adheres to all building requirements in the region where its data centers are located. More details can be found in Google's Security Whitepaper: https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers Google adheres to all building and facility requirements in the region where its data centers are located.
F32	Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001:2013, Annex A.11). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Environmental health and safety controls are implemented at all Google Data Centers. All sites provide robust detection of environmental elements, including heat, fire, smoke and water detection. All sites provide robust fire protection, detection and prevention. Fire detection and suppression equipment helps prevent damage to hardware. Heat, fire, smoke, and water detectors trigger audible and visible alarms in the affected zone, at security operations consoles, and at remote monitoring desks. Google adheres to all building requirements in the region where its data centers are located. More details can be found in Google's Security Whitepaper: https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers Google adheres to all building and facility requirements in the region where its data centers are located.
F33	Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001:2013, Annex A.11). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Environmental health and safety controls are implemented at all Google Data Centers. Google maintains an ESD program that includes training to applicable standards as well as prevention of ESD throughout the data center. More details can be found in Google's Security Whitepaper: https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers Google adheres to all building and facility requirements in the region where its data centers are located.
F34	Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001:2013, Annex A.11). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Environment health and safety controls are implemented at all Google Data Centers. All sites provide robust fire protection, detection and prevention. Fire detection and suppression equipment helps prevent damage to hardware. Heat, fire, and smoke detectors trigger audible and visible alarms in the affected zone, at security operations consoles, and at remote monitoring desks. Google adheres to all building requirements in the region where its data centers are located. More details can be found in Google's Security Whitepaper: https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers Google adheres to all building and facility requirements in the region where its data centers are located.
F35	Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001:2013, Annex A.11). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. To keep things running 24/7 and ensure uninterrupted services Google's data centers feature redundant power systems and environmental controls. Every critical component has a primary and alternate power source, each with equal power. Diesel engine backup generators can provide enough emergency electrical power to run each data center at full capacity. Cooling systems maintain a constant operating temperature for servers and other hardware, reducing the risk of service outages. Fire detection and suppression equipment helps prevent damage to hardware. Heat, fire, and smoke detectors trigger audible and visible alarms in the affected zone, at security operations consoles, and at remote monitoring desks. Google adheres to all building requirements in the region where its data centers are located and maintains facilities that comply with best practices to minimize damage due to natural disasters. Google adheres to all building and facility requirements in the region where its data centers are located.

F36	Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001:2013, Annex A.11). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. To keep things running 24/7 and ensure uninterrupted services Google’s data centers feature redundant power systems and environmental controls. Every critical component has a primary and alternate power source, each with equal power. Diesel engine backup generators can provide enough emergency electrical power to run each data center at full capacity. Cooling systems maintain a constant operating temperature for servers and other hardware, reducing the risk of service outages. Fire detection and suppression equipment helps prevent damage to hardware. Heat, fire, and smoke detectors trigger audible and vis ble alarms in the affected zone, at security operations consoles, and at remote monitoring desks. Google adheres to all building and facility requirements in the region where its data centers are located and maintains facilities that comply with best practices to minimize damage due to natural disasters.
F37	Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001:2013, Annex A.11). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Environmental health and safety controls are implemented at all Google Data Centers. All sites provide robust fire protection, detection and prevention. Fire detection and suppression equipment helps prevent damage to hardware. Heat, fire, and smoke detectors trigger audible and visible alarms in the affected zone, at security operations consoles, and at remote monitoring desks. Google adheres to all building requirements in the region where its data centers are located. More details can be found in Google's Security Whitepaper: https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers Google adheres to all building and facility requirements in the region where its data centers are located.
F38	Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001:2013, Annex A.11). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Environmental health and safety controls are implemented at all Google Data Centers. All sites provide robust fire protection, detection and prevention. Fire detection and suppression equipment helps prevent damage to hardware. Heat, fire, and smoke detectors trigger aud ble and visible alarms in the affected zone, at security operations consoles, and at remote monitoring desks. Google adheres to all building requirements in the region where its data centers are located. More details can be found in Google's Security Whitepaper: https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers Google adheres to all building and facility requirements in the region where its data centers are located.
F39	Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001:2013, Annex A.11). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Environmental health and safety controls are implemented at all Google Data Centers. All sites provide robust fire protection, detection and prevention. Fire detection and suppression equipment helps prevent damage to hardware. Heat, fire, and smoke detectors trigger audible and visible alarms in the affected zone, at security operations consoles, and at remote monitoring desks. Google adheres to all building requirements in the region where its data centers are located. More details can be found in Google's Security Whitepaper: https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers
F40	Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001:2013, Annex A.11). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Environmental health and safety controls are implemented at all Google Data Centers. All sites provide robust fire protection, detection and prevention. Fire detection and suppression equipment helps prevent damage to hardware. Heat, fire, and smoke detectors trigger audible and visible alarms in the affected zone, at security operations consoles, and at remote monitoring desks. Google adheres to all building requirements in the region where its data centers are located. More details can be found in Google's Security Whitepaper: https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers Google adheres to all building and facility requirements in the region where its data centers are located.
F41	Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001:2013, Annex A.11). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Environmental health and safety controls are implemented at all Google Data Centers. All sites provide robust fire protection, detection and prevention. Fire detection and suppression equipment helps prevent damage to hardware. Heat, fire, and smoke detectors trigger aud ble and visible alarms in the affected zone, at security operations consoles, and at remote monitoring desks. Google adheres to all building requirements in the region where its data centers are located. More details can be found in Google's Security Whitepaper: https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers Google adheres to all building and facility requirements in the region where its data centers are located.
F42	Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001:2013, Annex A.11). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Environmental health and safety controls are implemented at all Google Data Centers. All sites provide robust fire protection, detection and prevention. Fire detection and suppression equipment helps prevent damage to hardware. Heat, fire, and smoke detectors trigger audible and visible alarms in the affected zone, at security operations consoles, and at remote monitoring desks. Google adheres to all building requirements in the region where its data centers are located. More details can be found in Google's Security Whitepaper: https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers Google adheres to all building and facility requirements in the region where its data centers are located.
F43	Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001:2013, Annex A.11). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Environmental health and safety controls are implemented at all Google Data Centers. All sites provide robust detection of environmental elements, including heat, fire, smoke and water detection. All sites provide robust fire protection, detection and prevention. Fire detection and suppression equipment helps prevent damage to hardware. Heat, fire, smoke, and water detectors trigger audible and visible alarms in the affected zone, at security operations consoles, and at remote monitoring desks. Google adheres to all building requirements in the region where its data centers are located. More details can be found in Google's Security Whitepaper: https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers Google adheres to all building and facility requirements in the region where its data centers are located.
F44	Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001:2013, Annex A.11). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google applies data center controls based on risk, including risks related to the region the data center is located. Where applicable, appropriate measures are taken to ensure that monitoring and management of natural and environmental disasters is taken, and that teams are trained to respond to local events. Google adheres to all building and facility requirements in the region where its data centers are located.

F45	Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001:2013, Annex A.11). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Physical access to secured areas (such as the data server floor) is only possible via a security corridor. Google implements multi-factor access control using security badges and biometrics. Only approved employees with specific roles may enter secured areas, and all access to those area is monitored, logged and periodically approved for appropriateness. Google adheres to all building and facility requirements in the region where its data centers are located.
F46	Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001:2013, Annex A.11). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Environmental health and safety controls are implemented at all Google Data Centers. All sites provide robust detection of environmental elements, including heat, fire, smoke and water detection. All sites provide robust fire protection, detection and prevention. Fire detection and suppression equipment helps prevent damage to hardware. Heat, fire, smoke, and water detectors trigger audible and visible alarms in the affected zone, at security operations consoles, and at remote monitoring desks. Google adheres to all building requirements in the region where its data centers are located. More details can be found in Google's Security Whitepaper: https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers Google adheres to all building and facility requirements in the region where its data centers are located.
F47	Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001:2013, Annex A.11). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google applies data center controls based on risk, including risks related to the region the data center is located. Where applicable, appropriate measures are taken to ensure that monitoring and management of natural and environmental disasters is taken, and that teams are trained to respond to local events. Google adheres to all building and facility requirements in the region where its data centers are located.
F48	Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001:2013, Annex A.11). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Environmental health and safety controls are implemented at all Google Data Centers. All sites provide robust fire protection, detection and prevention. Fire detection and suppression equipment helps prevent damage to hardware. Heat, fire, and smoke detectors trigger audible and visible alarms in the affected zone, at security operations consoles, and at remote monitoring desks. Google adheres to all building requirements in the region where its data centers are located. More details can be found in Google's Security Whitepaper: https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers Google adheres to all building and facility requirements in the region where its data centers are located.
F49	Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001:2013, Annex A.11). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Environmental health and safety controls are implemented at all Google Data Centers. Google maintains an ESD program that includes training to applicable standards as well as prevention of ESD throughout the data center. More details can be found in Google's Security Whitepaper: https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers Google adheres to all building and facility requirements in the region where its data centers are located.
F50	Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001:2013, Annex A.11). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. To keep things running 24/7 and ensure uninterrupted services Google’s data centers feature redundant power systems and environmental controls. Every critical component has a primary and alternate power source, each with equal power. Diesel engine backup generators can provide enough emergency electrical power to run each data center at full capacity. Cooling systems maintain a constant operating temperature for servers and other hardware, reducing the risk of service outages. Fire detection and suppression equipment helps prevent damage to hardware. Heat, fire, and smoke detectors trigger audible and vis ble alarms in the affected zone, at security operations consoles, and at remote monitoring desks. Google adheres to all building and facility requirements in the region where its data centers are located and maintains facilities that comply with best practices to minimize damage due to natural disasters.
F51	Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001:2013, Annex A.11). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. To keep things running 24/7 and ensure uninterrupted services Google’s data centers feature redundant power systems and environmental controls. Every critical component has a primary and alternate power source, each with equal power. Diesel engine backup generators can provide enough emergency electrical power to run each data center at full capacity. Cooling systems maintain a constant operating temperature for servers and other hardware, reducing the risk of service outages. Fire detection and suppression equipment helps prevent damage to hardware. Heat, fire, and smoke detectors trigger audible and vis ble alarms in the affected zone, at security operations consoles, and at remote monitoring desks. Google adheres to all building and facility requirements in the region where its data centers are located and maintains facilities that comply with best practices to minimize damage due to natural disasters.
F52	Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001:2013, Annex A.11). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. To keep things running 24/7 and ensure uninterrupted services Google’s data centers feature redundant power systems and environmental controls. Every critical component has a primary and alternate power source, each with equal power. Diesel engine backup generators can provide enough emergency electrical power to run each data center at full capacity. Cooling systems maintain a constant operating temperature for servers and other hardware, reducing the risk of service outages. Fire detection and suppression equipment helps prevent damage to hardware. Heat, fire, and smoke detectors trigger audible and vis ble alarms in the affected zone, at security operations consoles, and at remote monitoring desks. Google adheres to all building and facility requirements in the region where its data centers are located and maintains facilities that comply with best practices to minimize damage due to natural disasters.
F53	Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001:2013, Annex A.11). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Environmental health and safety controls are implemented at all Google Data Centers. Employee safety is the most important of all consideration and appropriate signs are posted and training conducted to ensure all staff can safely evacuate in case of an emergency. All sites provide robust fire protection, detection and prevention. Fire detection and suppression equipment helps prevent damage to hardware. Heat, fire, and smoke detectors trigger aud ble and visible alarms in the affected zone, at security operations consoles, and at remote monitoring desks. More details can be found in Google's Security Whitepaper: https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers Google adheres to all building and facility requirements in the region where its data centers are located.
F54	Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001:2013, Annex A.11). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google designs the components of our platform to be highly redundant. This redundancy applies to our server design, how we store data, network and internet connectivity, and the software services themselves. This “redundancy of everything” includes the handling of errors by design and creates a solution that is not dependant on a single server, data center, or network connection. Google’s data centers are geographically distr buted to minimize the effects of regional disruptions such as natural disasters and local outages. In the event of hardware, software, or network failure, data is automatically shifted from one facility to another so that Google Cloud and G Suite customers can continue working in most cases without interruption. Google’s highly redundant infrastructure also helps protect our customers from data loss. For Google Cloud Products (G Suite and Google Cloud Platform), our Recovery Point Objective (RPO) target is zero, and our recovery time objective (RTO) design target is also zero. We aim to achieve these targets through live or synchronous replication: actions you take in Cloud products are simultaneously replicated in two data centers at once, so that if one data center fails, we transfer your data over to the other one that's also been reflecting your actions. Google adheres to all building and facility requirements in the region where its data centers are located.

F55	Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001:2013, Annex A.11). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Environmental health and safety controls are implemented at all Google Data Centers. All sites provide robust detection of environmental elements, including heat, fire, smoke and water detection. All sites provide robust fire protection, detection and prevention. Fire detection and suppression equipment helps prevent damage to hardware. Heat, fire, smoke, and water detectors trigger audible and visible alarms in the affected zone, at security operations consoles, and at remote monitoring desks. Google adheres to all building requirements in the region where its data centers are located. More details can be found in Google's Security Whitepaper: https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers Google adheres to all building and facility requirements in the region where its data centers are located.
F56	Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001:2013, Annex A.11). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Environmental health and safety controls are implemented at all Google Data Centers. All sites provide robust fire protection, detection and prevention. Fire detection and suppression equipment helps prevent damage to hardware. Heat, fire, and smoke detectors trigger audible and visible alarms in the affected zone, at security operations consoles, and at remote monitoring desks. Google adheres to all building requirements in the region where its data centers are located. More details can be found in Google's Security Whitepaper: https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers Google adheres to all building and facility requirements in the region where its data centers are located.
F57	Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001:2013, Annex A.11). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Environmental health and safety controls are implemented at all Google Data Centers. All sites provide robust fire protection, detection and prevention. Fire detection and suppression equipment helps prevent damage to hardware. Heat, fire, and smoke detectors trigger aud ble and visible alarms in the affected zone, at security operations consoles, and at remote monitoring desks. Google adheres to all building requirements in the region where its data centers are located. More details can be found in Google's Security Whitepaper: https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers Google adheres to all building and facility requirements in the region where its data centers are located.
F58	Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001:2013, Annex A.11). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Environmental health and safety controls are implemented at all Google Data Centers. All sites provide robust fire protection, detection and prevention. Fire detection and suppression equipment helps prevent damage to hardware. Heat, fire, and smoke detectors trigger aud ble and visible alarms in the affected zone, at security operations consoles, and at remote monitoring desks. Google adheres to all building requirements in the region where its data centers are located. More details can be found in Google's Security Whitepaper: https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers Google adheres to all building and facility requirements in the region where its data centers are located.
F59	Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001:2013, Annex A.11). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Environmental health and safety controls are implemented at all Google Data Centers. All sites provide robust detection of environmental elements, including heat, fire, smoke and water detection. All sites provide robust fire protection, detection and prevention. Fire detection and suppression equipment helps prevent damage to hardware. Heat, fire, smoke, and water detectors trigger audible and visible alarms in the affected zone, at security operations consoles, and at remote monitoring desks. Google adheres to all building requirements in the region where its data centers are located. More details can be found in Google's Security Whitepaper: https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers Google adheres to all building and facility requirements in the region where its data centers are located.
F60	Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001:2013, Annex A.11). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Environmental health and safety controls are implemented at all Google Data Centers. All sites provide robust fire protection, detection and prevention. Fire detection and suppression equipment helps prevent damage to hardware. Heat, fire, and smoke detectors trigger aud ble and visible alarms in the affected zone, at security operations consoles, and at remote monitoring desks. Google adheres to all building requirements in the region where its data centers are located. More details can be found in Google's Security Whitepaper: https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers Google adheres to all building and facility requirements in the region where its data centers are located.
F61	Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001:2013, Annex A.11). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. To keep things running 24/7 and ensure uninterrupted services Google's data centers feature redundant power systems and environmental controls. Every critical component has a primary and alternate power source, each with equal power. Diesel engine backup generators can provide enough emergency electrical power to run each data center at full capacity. Cooling systems maintain a constant operating temperature for servers and other hardware, reducing the risk of service outages. Fire detection and suppression equipment helps prevent damage to hardware. Heat, fire, and smoke detectors trigger audible and vis ble alarms in the affected zone, at security operations consoles, and at remote monitoring desks. Google adheres to all building and facility requirements in the region where its data centers are located.
F62	Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001:2013, Annex A.11). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. To keep things running 24/7 and ensure uninterrupted services Google's data centers feature redundant power systems and environmental controls. Every critical component has a primary and alternate power source, each with equal power. Diesel engine backup generators can provide enough emergency electrical power to run each data center at full capacity. Cooling systems maintain a constant operating temperature for servers and other hardware, reducing the risk of service outages. Fire detection and suppression equipment helps prevent damage to hardware. Heat, fire, and smoke detectors trigger audible and vis ble alarms in the affected zone, at security operations consoles, and at remote monitoring desks. Google adheres to all building and facility requirements in the region where its data centers are located.
F63	Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001:2013, Annex A.11). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. To keep things running 24/7 and ensure uninterrupted services Google's data centers feature redundant power systems and environmental controls. Every critical component has a primary and alternate power source, each with equal power. Diesel engine backup generators can provide enough emergency electrical power to run each data center at full capacity. Cooling systems maintain a constant operating temperature for servers and other hardware, reducing the risk of service outages. Fire detection and suppression equipment helps prevent damage to hardware. Heat, fire, and smoke detectors trigger audible and vis ble alarms in the affected zone, at security operations consoles, and at remote monitoring desks. Google adheres to all building and facility requirements in the region where its data centers are located.

F64	Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001:2013, Annex A.11). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. To keep things running 24/7 and ensure uninterrupted services Google’s data centers feature redundant power systems and environmental controls. Every critical component has a primary and alternate power source, each with equal power. Diesel engine backup generators can provide enough emergency electrical power to run each data center at full capacity. Cooling systems maintain a constant operating temperature for servers and other hardware, reducing the risk of service outages. Fire detection and suppression equipment helps prevent damage to hardware. Heat, fire, and smoke detectors trigger audible and vis ble alarms in the affected zone, at security operations consoles, and at remote monitoring desks. Google adheres to all building and facility requirements in the region where its data centers are located.
F65	Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001:2013, Annex A.11). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google applies data center controls based on risk, including risks related to the region the data center is located. Where applicable, appropriate measures are taken to ensure that monitoring and management of natural and environmental disasters is taken, and that teams are trained to respond to local events. To keep things running 24/7 and ensure uninterrupted services Google’s data centers feature redundant power systems and environmental controls. Every critical component has a primary and alternate power source, each with equal power. Diesel engine backup generators can provide enough emergency electrical power to run each data center at full capacity. Cooling systems maintain a constant operating temperature for servers and other hardware, reducing the risk of service outages. Fire detection and suppression equipment helps prevent damage to hardware. Heat, fire, and smoke detectors trigger audible and vis ble alarms in the affected zone, at security operations consoles, and at remote monitoring desks. Google adheres to all building and facility requirements in the region where its data centers are located.
F66	Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001:2013, Annex A.11). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. To keep things running 24/7 and ensure uninterrupted services Google’s data centers feature redundant power systems and environmental controls. Every critical component has a primary and alternate power source, each with equal power. Diesel engine backup generators can provide enough emergency electrical power to run each data center at full capacity. Cooling systems maintain a constant operating temperature for servers and other hardware, reducing the risk of service outages. Fire detection and suppression equipment helps prevent damage to hardware. Heat, fire, and smoke detectors trigger audible and vis ble alarms in the affected zone, at security operations consoles, and at remote monitoring desks. Google adheres to all building and facility requirements in the region where its data centers are located and maintains facilities that comply with best practices to minimize damage due to natural disasters.
F67	Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001:2013, Annex A.11). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. To keep things running 24/7 and ensure uninterrupted services Google’s data centers feature redundant power systems and environmental controls. Every critical component has a primary and alternate power source, each with equal power. Diesel engine backup generators can provide enough emergency electrical power to run each data center at full capacity. Cooling systems maintain a constant operating temperature for servers and other hardware, reducing the risk of service outages. Fire detection and suppression equipment helps prevent damage to hardware. Heat, fire, and smoke detectors trigger audible and vis ble alarms in the affected zone, at security operations consoles, and at remote monitoring desks. Google adheres to all building and facility requirements in the region where its data centers are located.
F68	Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001:2013, Annex A.11). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. To keep things running 24/7 and ensure uninterrupted services Google’s data centers feature redundant power systems and environmental controls. Every critical component has a primary and alternate power source, each with equal power. Diesel engine backup generators can provide enough emergency electrical power to run each data center at full capacity. Cooling systems maintain a constant operating temperature for servers and other hardware, reducing the risk of service outages. Fire detection and suppression equipment helps prevent damage to hardware. Heat, fire, and smoke detectors trigger audible and vis ble alarms in the affected zone, at security operations consoles, and at remote monitoring desks. Google adheres to all building and facility requirements in the region where its data centers are located.
F69	Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001:2013, Annex A.11). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. To keep things running 24/7 and ensure uninterrupted services Google’s data centers feature redundant power systems and environmental controls. Every critical component has a primary and alternate power source, each with equal power. Diesel engine backup generators can provide enough emergency electrical power to run each data center at full capacity. Cooling systems maintain a constant operating temperature for servers and other hardware, reducing the risk of service outages. Fire detection and suppression equipment helps prevent damage to hardware. Heat, fire, and smoke detectors trigger audible and vis ble alarms in the affected zone, at security operations consoles, and at remote monitoring desks. Google adheres to all building and facility requirements in the region where its data centers are located.
F70	Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001:2013, Annex A.11). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. To keep things running 24/7 and ensure uninterrupted services Google’s data centers feature redundant power systems and environmental controls. Every critical component has a primary and alternate power source, each with equal power. Diesel engine backup generators can provide enough emergency electrical power to run each data center at full capacity. Cooling systems maintain a constant operating temperature for servers and other hardware, reducing the risk of service outages. Fire detection and suppression equipment helps prevent damage to hardware. Heat, fire, and smoke detectors trigger audible and vis ble alarms in the affected zone, at security operations consoles, and at remote monitoring desks. Google adheres to all building and facility requirements in the region where its data centers are located.
F71	Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001:2013, Annex A.11). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. To keep things running 24/7 and ensure uninterrupted services Google’s data centers feature redundant power systems and environmental controls. Every critical component has a primary and alternate power source, each with equal power. Diesel engine backup generators can provide enough emergency electrical power to run each data center at full capacity. Cooling systems maintain a constant operating temperature for servers and other hardware, reducing the risk of service outages. Fire detection and suppression equipment helps prevent damage to hardware. Heat, fire, and smoke detectors trigger audible and vis ble alarms in the affected zone, at security operations consoles, and at remote monitoring desks. Google adheres to all building and facility requirements in the region where its data centers are located.
F72	Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001:2013, Annex A.11). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Cooling systems are installed and maintained per industry best practice. Google maintains a constant operating temperature for servers and other hardware, reducing the risk of service outages. Google adheres to all building and facility requirements in the region where its data centers are located.
F73	Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001:2013, Annex A.11). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Cooling systems are installed and maintained per industry best practice. Google maintains a constant operating temperature for servers and other hardware, reducing the risk of service outages. Google adheres to all building and facility requirements in the region where its data centers are located.
F74	Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001:2013, Annex A.11). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Cooling systems are installed and maintained per industry best practice. Google maintains a constant operating temperature for servers and other hardware, reducing the risk of service outages. Google adheres to all building and facility requirements in the region where its data centers are located.

F75	Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001:2013, Annex A.11). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google designs the components of our platform to be highly redundant. This redundancy applies to our server design, how we store data, network and internet connectivity, and the software services themselves. This “redundancy of everything” includes the handling of errors by design and creates a solution that is not dependant on a single server, data center, or network connection. Google’s data centers are geographically distributed to minimize the effects of regional disruptions such as natural disasters and local outages. In the event of hardware, software, or network failure, data is automatically shifted from one facility to another so that G Suite customers can continue working in most cases without interruption. Google’s highly redundant infrastructure also helps protect our customers from data loss. For Google Cloud Products (G Suite and Google Cloud Platform), our Recovery Point Objective (RPO) target is zero, and our recovery time objective (RTO) design target is also zero. We aim to achieve these targets through live or synchronous replication: actions you take in Cloud products are simultaneously replicated in two data centers at once, so that if one data center fails, we transfer your data over to the other one that's also been reflecting your actions. Google adheres to all building and facility requirements in the region where its data centers are located.
F76	Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001:2013, Annex A.11). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Cooling systems are installed and maintained per industry best practice. Google maintains a constant operating temperature for servers and other hardware, reducing the risk of service outages. Google adheres to all building and facility requirements in the region where its data centers are located.
F77	Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001:2013, Annex A.11). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google’s focus on security and protection of data is among our primary design criteria. Google data center physical security features a layered security model, including safeguards like custom-designed electronic access cards, alarms, vehicle access barriers, perimeter fencing, metal detectors, biometrics, and the data center floor features laser beam intrusion detection. Our data centers are monitored 24/7 by high-resolution interior and exterior cameras that can detect and track intruders. Access logs, activity records, and camera footage are available in case an incident occurs. Data centers are also routinely patrolled by experienced security guards who have undergone rigorous background checks and training. To learn more about our Data Center Processes, please see our Security Whitepaper and Data Center Introduction videos: Google Security Whitepaper: https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers Data Center Introduction Video: https://www.youtube.com/watch?v=XZmGGAbHqa0 Google adheres to all building and facility requirements in the region where its data centers are located.
F78	Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001:2013, Annex A.11). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. To keep things running 24/7 and ensure uninterrupted services Google’s data centers feature redundant power systems and environmental controls. Every critical component has a primary and alternate power source, each with equal power. Diesel engine backup generators can provide enough emergency electrical power to run each data center at full capacity. Cooling systems maintain a constant operating temperature for servers and other hardware, reducing the risk of service outages. Fire detection and suppression equipment helps prevent damage to hardware. Heat, fire, and smoke detectors trigger audible and visible alarms in the affected zone, at security operations consoles, and at remote monitoring desks. Google adheres to all building and facility requirements in the region where its data centers are located and maintains facilities that comply with best practices to minimize damage due to natural disasters.
F79	Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001:2013, Annex A.11). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Environmental health and safety controls are implemented at all Google Data Centers. All sites provide robust fire protection, detection and prevention. Fire detection and suppression equipment helps prevent damage to hardware. Heat, fire, and smoke detectors trigger audible and visible alarms in the affected zone, at security operations consoles, and at remote monitoring desks. Google adheres to all building requirements in the region where its data centers are located. Cooling systems are installed and maintained per industry best practice. Google maintains a constant operating temperature for servers and other hardware, reducing the risk of service outages. Google adheres to all building and facility requirements in the region where its data centers are located.
F80	Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001:2013, Annex A.11). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google’s focus on security and protection of data is among our primary design criteria. Google data center physical security features a layered security model, including safeguards like custom-designed electronic access cards, alarms, vehicle access barriers, perimeter fencing, metal detectors, biometrics, and the data center floor features laser beam intrusion detection. Our data centers are monitored 24/7 by high-resolution interior and exterior cameras that can detect and track intruders. Access logs, activity records, and camera footage are available in case an incident occurs. Data centers are also routinely patrolled by experienced security guards who have undergone rigorous background checks and training. To learn more about our Data Center Processes, please see our Security Whitepaper and Data Center Introduction videos: Google Security Whitepaper: https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers Data Center Introduction Video: https://www.youtube.com/watch?v=XZmGGAbHqa0 Google adheres to all building and facility requirements in the region where its data centers are located.
F81	Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001:2013, Annex A.11). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google’s focus on security and protection of data is among our primary design criteria. Google data center physical security features a layered security model, including safeguards like custom-designed electronic access cards, alarms, vehicle access barriers, perimeter fencing, metal detectors, biometrics, and the data center floor features laser beam intrusion detection. Our data centers are monitored 24/7 by high-resolution interior and exterior cameras that can detect and track intruders. Access logs, activity records, and camera footage are available in case an incident occurs. Data centers are also routinely patrolled by experienced security guards who have undergone rigorous background checks and training. To learn more about our Data Center Processes, please see our Security Whitepaper and Data Center Introduction videos: Google Security Whitepaper: https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers Data Center Introduction Video: https://www.youtube.com/watch?v=XZmGGAbHqa0 Google adheres to all building and facility requirements in the region where its data centers are located.
F82	Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001:2013, Annex A.11). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google’s focus on security and protection of data is among our primary design criteria. Google data center physical security features a layered security model, including safeguards like custom-designed electronic access cards, alarms, vehicle access barriers, perimeter fencing, metal detectors, biometrics, and the data center floor features laser beam intrusion detection. Our data centers are monitored 24/7 by high-resolution interior and exterior cameras that can detect and track intruders. Access logs, activity records, and camera footage are available in case an incident occurs. Data centers are also routinely patrolled by experienced security guards who have undergone rigorous background checks and training. To learn more about our Data Center Processes, please see our Security Whitepaper and Data Center Introduction videos: Google Security Whitepaper: https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers Data Center Introduction Video: https://www.youtube.com/watch?v=XZmGGAbHqa0 Google adheres to all building and facility requirements in the region where its data centers are located.

F83	Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001:2013, Annex A.11). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google's focus on security and protection of data is among our primary design criteria. Google data center physical security features a layered security model, including safeguards like custom-designed electronic access cards, alarms, vehicle access barriers, perimeter fencing, metal detectors, biometrics, and the data center floor features laser beam intrusion detection. Our data centers are monitored 24/7 by high-resolution interior and exterior cameras that can detect and track intruders. Access logs, activity records, and camera footage are available in case an incident occurs. Data centers are also routinely patrolled by experienced security guards who have undergone rigorous background checks and training. To learn more about our Data Center Processes, please see our Security Whitepaper and Data Center Introduction videos: Google Security Whitepaper: https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers Data Center Introduction Video: https://www.youtube.com/watch?v=XZmGGAbHqa0 Google adheres to all building and facility requirements in the region where its data centers are located.
F83-1	Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001:2013, Annex A.11). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google's focus on security and protection of data is among our primary design criteria. Google data center physical security features a layered security model, including safeguards like custom-designed electronic access cards, alarms, vehicle access barriers, perimeter fencing, metal detectors, biometrics, and the data center floor features laser beam intrusion detection. Our data centers are monitored 24/7 by high-resolution interior and exterior cameras that can detect and track intruders. Access logs, activity records, and camera footage are available in case an incident occurs. Data centers are also routinely patrolled by experienced security guards who have undergone rigorous background checks and training. To learn more about our Data Center Processes, please see our Security Whitepaper and Data Center Introduction videos: Google Security Whitepaper: https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers Data Center Introduction Video: https://www.youtube.com/watch?v=XZmGGAbHqa0 Google adheres to all building and facility requirements in the region where its data centers are located.
F84	Out of Scope
F85	Out of Scope
F86	Out of Scope
F87	Out of Scope
F88	Out of Scope
F89	Out of Scope
F90	Out of Scope
F91	Out of Scope
F92	Out of Scope
F93	Out of Scope
F94	Out of Scope
F95	Out of Scope
F96	Out of Scope
F97	Out of Scope
F98	Out of Scope
F99	Out of Scope
F100	Out of Scope
F101	Out of Scope
F102	Out of Scope
F103	Out of Scope
F104	Out of Scope
F105	Out of Scope
F106	Out of Scope
F107	Out of Scope
F108	Out of Scope
F109	Out of Scope
F110	Out of Scope
F111	Out of Scope
F112	Out of Scope
F113	Out of Scope
F114	Out of Scope
F115	Out of Scope
F116	Out of Scope
F117	Out of Scope
F118	Out of Scope
F119	Out of Scope
F120	Out of Scope
F121	Out of Scope
F122	Out of Scope
F123	Out of Scope
F124	Out of Scope
F125	Out of Scope
F126	Out of Scope
F127	Out of Scope
F128	Out of Scope
F129	Out of Scope
F130	Out of Scope
F131	Out of Scope
F132	Out of Scope
F133	Out of Scope
F134	Out of Scope
F135	Out of Scope
F136	Out of Scope
F137	Out of Scope
Operational	
Item No.	**Google Response**
O1	Google is certified to the ISO27001 Standard, which regulates "Information Security Policy" (ISO 27002:2013, Annex A.5) and Organization of Information Security (ISO27002:2013, Annex A.6). Information security oversight and management controls, including documentation of information security policies are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Customers using Google Cloud Platform retain all rights and responsibilities to configure and manage their environment.
O2	Google is certified to the ISO27001 Standard, which regulates "Information Security Policy" (ISO 27002:2013, Annex A.5) and Organization of Information Security (ISO27002:2013, Annex A.6). Information security oversight and management controls, including documentation of information security policies are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Customers using Google Cloud Platform retain all rights and responsibilities to configure and manage their environment.

O3	Google is certified to the ISO27001 Standard, which regulates "Information Security Policy" (ISO 27002:2013, Annex A.5) and Organization of Information Security (ISO27002:2013, Annex A.6). Information security oversight and management controls, including documentation of information security policies are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Customers using Google Cloud Platform retain all rights and respons bilities to configure and manage their environment.
O4	Google is certified to the ISO27001 Standard, which regulates "Information Security Policy" (ISO 27002:2013, Annex A.5) and Organization of Information Security (ISO27002:2013, Annex A.6). Information security oversight and management controls, including documentation of information security policies are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Customers using Google Cloud Platform retain all rights and respons bilities to configure and manage their environment.
O5	Google is certified to the ISO27001 Standard, which regulates "Information Security Policy" (ISO 27002:2013, Annex A.5) and Organization of Information Security (ISO27002:2013, Annex A.6). Information security oversight and management controls, including documentation of information security policies are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Customers using Google Cloud Platform retain all rights and respons bilities to configure and manage their environment.
O6	Google is certified to the ISO27001 Standard, which regulates "Information Security Policy" (ISO 27002:2013, Annex A.5) and Organization of Information Security (ISO27002:2013, Annex A.6). Information security oversight and management controls, including documentation of information security policies are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Customers using Google Cloud Platform retain all rights and respons bilities to configure and manage their environment.
O7	Google is certified to the ISO27001 Standard, which regulates "Redundancies" (ISO27001:2013, Annex A.17.2). Controls relating to availability and integrity of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google designs the components of our platform to be highly redundant. This redundancy applies to our server design, how we store data, network and internet connectivity, and the software services themselves. This "redundancy of everything" includes the handling of errors by design and creates a solution that is not dependant on a single server, data center, or network connection. Google's data centers are geographically distr buted to minimize the effects of regional disruptions such as natural disasters and local outages. In the event of hardware, software, or network failure, data is automatically shifted from one facility to another so that Google Cloud and G Suite customers can continue working in most cases without interruption. Google's highly redundant infrastructure also helps protect our customers from data loss. For Google Cloud Products (G Suite and Google Cloud Platform), our Recovery Point Objective (RPO) target is zero, and our recovery time objective (RTO) design target is also zero. We aim to achieve these targets through live or synchronous replication: actions you take in Cloud products are simultaneously replicated in two data centers at once, so that if one data center fails, we transfer your data over to the other one that's also been reflecting your actions. Customers using Google Cloud Platform retain all rights and respons bilities to configure and manage their environment, including configuring appropriate regions and zones to prevent failures or disasters.
O8	Google is certified to the ISO27001 Standard, which regulates "Human Resources Security" (ISO27001:2013, Annex A.7). Controls relating to human resource management are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. All employees agree to Google's Code of Conduct (https://abc.xyz/investor/other/google-code-of-conduct.html) and recieve training on Ethics and Compliance topics. Customers using Google Cloud Platform retain all rights and respons bilities to configure and manage their environment, including development of operational guidance.
O9	Google is certified to the ISO27001 Standard, which regulates "Human Resources Security" (ISO27001:2013, Annex A.7). Controls relating to human resource management are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. All employees agree to Google's Code of Conduct (https://abc.xyz/investor/other/google-code-of-conduct.html) and recieve training on Ethics and Compliance topics. For customers using our Google Cloud Platform, they retain all rights and responsibilities to configure and manage their environment, including development of operational guidance.
O10	Google is certified to the ISO27001 Standard, which regulates "Information Security Policy" (ISO 27001:2013, Annex A.5), Organization of Information Security (ISO27001:2013, Annex A.6) and Operational Procedures and Responsibilities (ISO 27001:2013, Annex A 12.1) Information security oversight and management controls, including documentation of information security policies are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Customers using Google Cloud Platform retain all rights and respons bilities to configure and manage their environment, including development of operational guidance.
O10-1	Google is certified to the ISO27001 Standard, which regulates ""Information security awareness, education and training" (ISO 27001:2013, Annex A.7.2.2), Information security oversight and management controls, including management of security awareness and training are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. All Google employees undergo security training as part of the orientation process and receive ongoing security training throughout their Google careers. During orientation, new employees agree to our Code of Conduct, which highlights our commitment to keep customer information safe and secure. Depending on their job role, additional training on specific aspects of security may be required. For instance, the information security team instructs new engineers on topics l ke secure coding practices, product design and automated vulnerability testing tools. Engineers also attend technical presentations on security-related topics and receive a security newsletter that covers new threats, attack patterns, mitigation techniques and more. Customers using Google Cloud Platform retain all rights and respons bilities to configure and manage their environment, including development of operational guidance.
O11	Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001:2013, Annex A.11). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google's focus on security and protection of data is among our primary design criteria. Google data center physical security features a layered security model, including safeguards l ke custom-designed electronic access cards, alarms, vehicle access barriers, perimeter fencing, metal detectors, biometrics, and the data center floor features laser beam intrusion detection. Our data centers are monitored 24/7 by high-resolution interior and exterior cameras that can detect and track intruders. Access logs, activity records, and camera footage are available in case an incident occurs. Data centers are also routinely patrolled by experienced security guards who have undergone rigorous background checks and training. Physical access to secured areas (such as the data server floor) is only possible via a security corridor. Google implements multi-factor access control using security badges and biometrics. Only approved employees with specific roles may enter secured areas, and all access to those area is monitored and logged. To learn more about our Data Center Processes, please see our Security Whitepaper and Data Center Introduction videos: Google Security Whitepaper: https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers Data Center Introduction Video: https://www.youtube.com/watch?v=XZmGGAbHqa0

O12	Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001:2013, Annex A.11). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google's focus on security and protection of data is among our primary design criteria. Google data center physical security features a layered security model, including safeguards l ke custom-designed electronic access cards, alarms, vehicle access barriers, perimeter fencing, metal detectors, biometrics, and the data center floor features laser beam intrusion detection. Our data centers are monitored 24/7 by high-resolution interior and exterior cameras that can detect and track intruders. Access logs, activity records, and camera footage are available in case an incident occurs. Data centers are also routinely patrolled by experienced security guards who have undergone rigorous background checks and training. Physical access to secured areas (such as the data server floor) is only possible via a security corridor. Google implements multi-factor access control using security badges and biometrics. Only approved employees with specific roles may enter secured areas, and all access to those area is monitored and logged. To learn more about our Data Center Processes, please see our Security Whitepaper and Data Center Introduction videos: Google Security Whitepaper: https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers Data Center Introduction Video: https://www.youtube.com/watch?v=XZmGGAbHqa0
O13	"Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001:2013, Annex A.11). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google's focus on security and protection of data is among our primary design criteria. Google data center physical security features a layered security model, including safeguards l ke custom-designed electronic access cards, alarms, vehicle access barriers, perimeter fencing, metal detectors, biometrics, and the data center floor features laser beam intrusion detection. Our data centers are monitored 24/7 by high-resolution interior and exterior cameras that can detect and track intruders. Access logs, activity records, and camera footage are available in case an incident occurs. Data centers are also routinely patrolled by experienced security guards who have undergone rigorous background checks and training. Physical access to secured areas (such as the data server floor) is only possible via a security corridor. Google implements multi-factor access control using security badges and biometrics. Only approved employees with specific roles may enter secured areas, and all access to those area is monitored and logged. To learn more about our Data Center Processes, please see our Security Whitepaper and Data Center Introduction videos: Google Security Whitepaper: https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers Data Center Introduction Video: https://www.youtube.com/watch?v=XZmGGAbHqa0"
O14	Google is certified to the ISO27001 Standard, which regulates "Documented Operating Procedures" (Annex A.12.1.1). Google maintains robust internal documentation and maintains an ISMS, per ISO27001 requirements. All documentation in on systems that are replicated and subject to backup. Customers using Google Cloud Platform, retain all rights and responsibilities to configure and manage their environment, including development of operational guidance.
O15	Google is certified to the ISO27001 Standard, which regulates "Protection of Records" (Annex A.12.1.1) and "Information Security Aspects of Business Continuity Management" (Annex A.17). Google maintains operational documentation to facilitate the recovery of systems. Documentation is located on systems that are replicated and subject to backup. Customers using Google Cloud Platform retain all rights and respons bilities to configure and manage their environment, including development of operational guidance.
O16	Google is certified to the ISO27001 Standard, which regulates "Access Control" (ISO 27001:2013, Annex A.9). Information security oversight and management controls, including logical access controls are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. To keep data private and secure, Google logically isolates each customer's data from that of other customers and users, even when it's stored on the same physical server. Only a small group of Google employees have access to customer data. For Google employees, access rights and levels are based on an their job function and role, using the concepts of least–privilege and need–to–know to match access privileges to defined respons bilities. Google employees are only granted a limited set of default permissions to access company resources, such as employee email and Google's internal employee portal. Requests for additional access follow a formal process that involves a request and an approval from a data or system owner, manager, or other executives, as dictated by Google's security policies. Approvals are managed by workflow tools that maintain audit records of all changes. These tools control both the modification of authorization settings and the approval process to ensure consistent application of the approval policies. An employee's authorization settings are used to control access to all resources, including data and systems for Google Cloud and G Suite products. Support services are only provided to authorized customer administrators whose identities have been verified in several ways. Googler access is monitored and audited by our dedicated security, privacy, and internal audit teams Customers using Google Cloud Platform retain all rights and respons bilities to configure and manage their environment, including developing guidance for access to operational documentation.
O17	Google is certified to the ISO27001 Standard, which regulates "Access Control" (ISO 27001:2013, Annex A.9). Information security oversight and management controls, including logical access controls are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google implements secure multi-factor login procedures. As part of security training, users are educated on proper password creation and management. Further, Google has implemented a password management system to ensure compliance with internal policies. Customers using Google Cloud Platform retain all rights and respons bilities to configure and manage their environment, including developing guidance for access to operational documentation.
O18	Google is certified to the ISO27001 Standard, which regulates "Access Control" (ISO 27001:2013, Annex A.9). Information security oversight and management controls, including logical access controls are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google periodically reviews logical access to all systems to ensure appropriateness of access. Further, Googler access is monitored and audited by our dedicated security, privacy, and internal audit teams. Customers using Google Cloud Platform retain all rights and respons bilities to configure and manage their environment, including developing guidance for access to operational documentation.
O19	Google is certified to the ISO27001 Standard, which regulates "Access Control" (ISO 27001:2013, Annex A.9). Information security oversight and management controls, including logical access controls are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. For Google employees, access rights and levels are based on an their job function and role, using the concepts of least–privilege and need–to–know to match access privileges to defined respons bilities. Google employees are only granted a limited set of default permissions to access company resources, such as employee email and Google's internal employee portal. Requests for additional access follow a formal process that involves a request and an approval from a data or system owner, manager, or other executives, as dictated by Google's security policies. Approvals are managed by workflow tools that maintain audit records of all changes. These tools control both the modification of authorization settings and the approval process to ensure consistent application of the approval policies. An employee's authorization settings are used to control access to all resources, including data and systems for Google Cloud and G Suite products. Support services are only provided to authorized customer administrators whose identities have been verified in several ways. Googler access is monitored and audited by our dedicated security, privacy, and internal audit teams. Customers using Google Cloud Platform retain all rights and respons bilities to configure and manage their environment, including developing guidance for access to operational documentation.

O20	Google is certified to the ISO27001 Standard, which regulates "Access Control" (ISO 27001:2013, Annex A.9). Information security oversight and management controls, including logical access controls are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. For Google employees, access rights and levels are based on an their job function and role, using the concepts of least–privilege and need–to–know to match access privileges to defined respons bilities. Google employees are only granted a limited set of default permissions to access company resources, such as employee email and Google's internal employee portal. Requests for additional access follow a formal process that involves a request and an approval from a data or system owner, manager, or other executives, as dictated by Google's security policies. Approvals are managed by workflow tools that maintain audit records of all changes. These tools control both the modification of authorization settings and the approval process to ensure consistent application of the approval policies. An employee's authorization settings are used to control access to all resources, including data and systems for Google Cloud and G Suite products. Support services are only provided to authorized customer administrators whose identities have been verified in several ways. Googler access is monitored and audited by our dedicated security, privacy, and internal audit teams. Customers using Google Cloud Platform retain all rights and respons bilities to configure and manage their environment, including developing guidance for access to operational documentation.
O21	Google is certified to the ISO27001 Standard, which regulates "Access Control" (ISO 27001:2013, Annex A.9). Information security oversight and management controls, including logical access controls are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. For Google employees, access rights and levels are based on an their job function and role, using the concepts of least–privilege and need–to–know to match access privileges to defined respons bilities. Google employees are only granted a limited set of default permissions to access company resources, such as employee email and Google's internal employee portal. Requests for additional access follow a formal process that involves a request and an approval from a data or system owner, manager, or other executives, as dictated by Google's security policies. Approvals are managed by workflow tools that maintain audit records of all changes. These tools control both the modification of authorization settings and the approval process to ensure consistent application of the approval policies. An employee's authorization settings are used to control access to all resources, including data and systems for Google Cloud and G Suite products. Support services are only provided to authorized customer administrators whose identities have been verified in several ways. Googler access is monitored and audited by our dedicated security, privacy, and internal audit teams. Customers using Google Cloud Platform retain all rights and respons bilities to configure and manage their environment, including developing guidance for access to operational documentation.
O22	Google is certified to the ISO27001 Standard, which regulates "Access Control" (ISO 27001:2013, Annex A.9). Information security oversight and management controls, including logical access controls are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. For Google employees, access rights and levels are based on an their job function and role, using the concepts of least–privilege and need–to–know to match access privileges to defined respons bilities. Google employees are only granted a limited set of default permissions to access company resources, such as employee email and Google's internal employee portal. Requests for additional access follow a formal process that involves a request and an approval from a data or system owner, manager, or other executives, as dictated by Google's security policies. Approvals are managed by workflow tools that maintain audit records of all changes. These tools control both the modification of authorization settings and the approval process to ensure consistent application of the approval policies. An employee's authorization settings are used to control access to all resources, including data and systems for Google Cloud and G Suite products. Support services are only provided to authorized customer administrators whose identities have been verified in several ways. Googler access is monitored and audited by our dedicated security, privacy, and internal audit teams. Customers using Google Cloud Platform retain all rights and respons bilities to configure and manage their environment, including developing guidance for access to operational documentation.
O23	Google is certified to the ISO27001 Standard, which regulates "Access Control" (ISO 27001:2013, Annex A.9). Information security oversight and management controls, including logical access controls are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. For Google employees, access rights and levels are based on an their job function and role, using the concepts of least–privilege and need–to–know to match access privileges to defined respons bilities. Google employees are only granted a limited set of default permissions to access company resources, such as employee email and Google's internal employee portal. Requests for additional access follow a formal process that involves a request and an approval from a data or system owner, manager, or other executives, as dictated by Google's security policies. Approvals are managed by workflow tools that maintain audit records of all changes. These tools control both the modification of authorization settings and the approval process to ensure consistent application of the approval policies. An employee's authorization settings are used to control access to all resources, including data and systems for Google Cloud and G Suite products. Support services are only provided to authorized customer administrators whose identities have been verified in several ways. Googler access is monitored and audited by our dedicated security, privacy, and internal audit teams. Customers using Google Cloud Platform retain all rights and respons bilities to configure and manage their environment, including developing guidance for access to operational documentation.
O24	Google is certified to the ISO27001 Standard, which regulates "System Acquisition, Development and Maintenance" (ISO 27001:2013, Annex A.14). Information security oversight and management controls, including software development controls are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Customers using Google Cloud Platform retain all rights and respons bilities to configure and manage their environment, including developing a process to support input management activities.
O25	Google is certified to the ISO27001 Standard, which regulates "System Acquisition, Development and Maintenance" (ISO 27001:2013, Annex A.14). Information security oversight and management controls, including software development controls are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Customers using Google Cloud Platform retain all rights and respons bilities to configure and manage their environment, including developing a process to support input management activities.
O26	Google is certified to the ISO27001 Standard, which regulates "System Acquisition, Development and Maintenance" (ISO 27001:2013, Annex A.14). Information security oversight and management controls, including software development controls are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Customers using Google Cloud Platform retain all rights and respons bilities to configure and manage their environment, including developing a process to support input management activities.
O27	Google is certified to the ISO27001 Standard, which regulates "Redundancies" (ISO27001:2013, Annex A.17.2) and "Backup" (ISO27001:2013 Annex A 12.3.) Controls relating to availability and integrity of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google designs the components of our platform to be highly redundant. This redundancy applies to our server design, how we store data, network and internet connectivity, and the software services themselves. This "redundancy of everything" includes the handling of errors by design and creates a solution that is not dependant on a single server, data center, or network connection. Google's data centers are geographically distr buted to minimize the effects of regional disruptions such as natural disasters and local outages. In the event of hardware, software, or network failure, data is automatically shifted from one facility to another so that Google Cloud and G Suite customers can continue working in most cases without interruption. Google's highly redundant infrastructure also helps protect our customers from data loss. For Google Cloud Products (G Suite and Google Cloud Platform), our Recovery Point Objective (RPO) target is zero, and our recovery time objective (RTO) design target is also zero. We aim to achieve these targets through live or synchronous replication: actions you take in Cloud products are simultaneously replicated in two data centers at once, so that if one data center fails, we transfer your data over to the other one that's also been reflecting your actions. Customers using Google Cloud Platform retain all rights and respons bilities to configure and manage their environment, including developing a process to support data file management activities.
O28	Google is certified to the ISO27001 Standard, which regulates "System Acquisition, Development and Maintenance" (ISO 27001:2013, Annex A.14). Information security oversight and management controls, including software development controls are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Customers using Google Cloud Platform retain all rights and respons bilities to configure and manage their environment, including developing a process to support program file management activities.

O29	Google is certified to the ISO27001 Standard, which regulates "Redundancies" (ISO27001:2013, Annex A.17.2) and "Backup" (ISO27001:2013 Annex A 12.3.) Controls relating to availability and integrity of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google designs the components of our platform to be highly redundant. This redundancy applies to our server design, how we store data, network and internet connectivity, and the software services themselves. This “redundancy of everything” includes the handling of errors by design and creates a solution that is not dependant on a single server, data center, or network connection. Google’s data centers are geographically distr buted to minimize the effects of regional disruptions such as natural disasters and local outages. In the event of hardware, software, or network failure, data is automatically shifted from one facility to another so that Google Cloud and G Suite customers can continue working in most cases without interruption. Google’s highly redundant infrastructure also helps protect our customers from data loss. For Google Cloud Products (G Suite and Google Cloud Platform), our Recovery Point Objective (RPO) target is zero, and our recovery time objective (RTO) design target is also zero. We aim to achieve these targets through live or synchronous replication: actions you take in Cloud products are simultaneously replicated in two data centers at once, so that if one data center fails, we transfer your data over to the other one that's also been reflecting your actions. Customers using Google Cloud Platform retain all rights and respons bilities to configure and manage their environment, including developing a process to support program file management activities.
O30	Google is certified to the ISO27001 Standard, which regulates "Protection from Malware" (Annex A.12.2). Controls relating to vulnerability management are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google administers a vulnerability management process that actively scans for security threats using a combination of commercially available and purpose-built in house tools, intensive automated and manual penetration efforts, quality assurance processes, software security reviews and external audits. The vulnerability management team is respons ble for tracking and following up on vulnerabilities. Once a vulnerability requiring remediation has been identified, it is logged, prioritized according to severity, and assigned an owner. The vulnerability management team tracks such issues and follows up frequently until they can verify that the issues have been remediated. Google also maintains relationships and interfaces with members of the security research community to track reported issues in Google services and open source tools. More information about reporting security issues can be found at www.google.com/intl/en/corporate/security.html. Customers using Google Cloud Platform retain all rights and respons bilities to configure and manage their environment, including configuring appropriate protective measures against viruses.
O31	"Google is certified to the ISO27001 Standards, which regulates "Operational Procedures and Responsibilities" (ISO 27001:2013, Annex A.12.1) and "Network Security" (ISO 27001:2013, Annex A.13.1). Google’s security monitoring program is focused on information gathered from internal network traffic, employee actions on systems and outside knowledge of vulnerabilities. At many points across our global network, internal traffic is inspected for suspicious behavior, such as the presence of traffic that might indicate botnet connections. This analysis is performed using a combination of open source and commercial tools for traffic capture and parsing. A proprietary correlation system built on top of Google technology also supports this analysis. Network analysis is supplemented by examining system logs to identify unusual behavior, such as attempted access of customer data. Google security engineers place standing search alerts on public data repositories to look for security incidents that might affect the company’s infrastructure. They actively review inbound security reports and monitor public mailing lists, blog posts, and wikis. Automated network analysis helps determine when an unknown threat may exist and escalates to Google security staff, and network analysis is supplemented by automated analysis of system logs. Customers using Google Cloud Platform retain all rights and respons bilities to configure and manage their environment.
O32	Google is certified to the ISO27001 Standard, which regulates "Redundancies" (ISO27001:2013, Annex A.17.2) and "Backup" (ISO27001:2013 Annex A 12.3.) Controls relating to availability and integrity of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google designs the components of our platform to be highly redundant. This redundancy applies to our server design, how we store data, network and internet connectivity, and the software services themselves. This “redundancy of everything” includes the handling of errors by design and creates a solution that is not dependant on a single server, data center, or network connection. Google’s data centers are geographically distr buted to minimize the effects of regional disruptions such as natural disasters and local outages. In the event of hardware, software, or network failure, data is automatically shifted from one facility to another so that Google Cloud and G Suite customers can continue working in most cases without interruption. Google’s highly redundant infrastructure also helps protect our customers from data loss. For Google Cloud Products (G Suite and Google Cloud Platform), our Recovery Point Objective (RPO) target is zero, and our recovery time objective (RTO) design target is also zero. We aim to achieve these targets through live or synchronous replication: actions you take in Cloud products are simultaneously replicated in two data centers at once, so that if one data center fails, we transfer your data over to the other one that's also been reflecting your actions. Customers using Google Cloud Platform retain all rights and respons bilities to configure and manage their environment, including configuring appropriate regions and zones to prevent failures or disasters.
O33	Google is certified to the ISO27001 Standard, which regulates "Protection of Records" (ISO 27001:2013, Annex A.12.1.1). Customers using Google Cloud Platform retain all rights and respons bilities to configure and manage their environment, including developing a process to support storage management.
O34	Google is certified to the ISO27001 Standard, which regulates "Redundancies" (ISO27001:2013, Annex A.17.2) and "Backup" (ISO27001:2013 Annex A 12.3.) Controls relating to availability and integrity of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google designs the components of our platform to be highly redundant. This redundancy applies to our server design, how we store data, network and internet connectivity, and the software services themselves. This “redundancy of everything” includes the handling of errors by design and creates a solution that is not dependant on a single server, data center, or network connection. Google’s data centers are geographically distr buted to minimize the effects of regional disruptions such as natural disasters and local outages. In the event of hardware, software, or network failure, data is automatically shifted from one facility to another so that Google Cloud and G Suite customers can continue working in most cases without interruption. Google’s highly redundant infrastructure also helps protect our customers from data loss. For Google Cloud Products (G Suite and Google Cloud Platform), our Recovery Point Objective (RPO) target is zero, and our recovery time objective (RTO) design target is also zero. We aim to achieve these targets through live or synchronous replication: actions you take in Cloud products are simultaneously replicated in two data centers at once, so that if one data center fails, we transfer your data over to the other one that's also been reflecting your actions. Customers using Google Cloud Platform retain all rights and responsibilities to configure and manage their environment, including developing a process to support forms management.
O35	Responsibility for developing a process to support forms management rests with the customer.
O36	Responsibility for developing a process to support forms management rests with the customer.
O37	Responsibility for developing a process to support output information rests with the customer.
O38	Responsibility for transaction management rests with the customer.
O39	Responsibility for transaction management rests with the customer.
O40	Responsibility for transaction management rests with the customer.
O41	Responsibility for transaction management rests with the customer.
O42	Responsibility for transaction management rests with the customer.
O43	Google is certified to the ISO27001 Standard, which regulates "Cryptography" (ISO 27001:2013, Annex A.10) Google publishes details about encryption and key management options for its Google Cloud and G Suite products. To read more about key management and encryption, please see: https://cloud.google.com/security/encryption-at-rest/ https://storage.googleapis.com/gfw-touched-accounts-pdfs/google-encryption-whitepaper-G Suite.pdf Customers using Google Cloud Platform retain all rights and respons bilities to configure and manage their environment, including developing cryptographic key management processes.
O44	Responsibility for validation of identity rests with the customer.
O44-1	Responsibility for validation of cash transactions via CD/ATM rest with the customer.
O45	Responsibility for CD/ATM and unmanned branches rests with the customer.
O46	Responsibility for CD/ATM and unmanned branches rests with the customer.
O47	Responsibility for CD/ATM and unmanned branches rests with the customer.
O48	Responsibility for CD/ATM and unmanned branches rests with the customer.
O49	Responsibility for CD/ATM and unmanned branches rests with the customer.
O50	Responsibility for handheld terminals rests with the customer.
O51	Responsibility for CD/ATM and unmanned branches rests with the customer.
O51-1	Responsibility for CD/ATM and unmanned branches rests with the customer.
O52	Responsibility for CD/ATM and unmanned branches rests with the customer.

O53	Google is certified to the ISO27001 Standard, which regulates "Redundancies" (ISO27001:2013, Annex A.17.2) and "Backup" (ISO27001:2013 Annex A 12.3.) Controls relating to availability and integrity of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google designs the components of our platform to be highly redundant. This redundancy applies to our server design, how we store data, network and internet connectivity, and the software services themselves. This "redundancy of everything" includes the handling of errors by design and creates a solution that is not dependant on a single server, data center, or network connection. Google's data centers are geographically distr buted to minimize the effects of regional disruptions such as natural disasters and local outages. In the event of hardware, software, or network failure, data is automatically shifted from one facility to another so that Google Cloud and G Suite customers can continue working in most cases without interruption. Google's highly redundant infrastructure also helps protect our customers from data loss. For Google Cloud Products (G Suite and Google Cloud Platform), our Recovery Point Objective (RPO) target is zero, and our recovery time objective (RTO) design target is also zero. We aim to achieve these targets through live or synchronous replication: actions you take in Cloud products are simultaneously replicated in two data centers at once, so that if one data center fails, we transfer your data over to the other one that's also been reflecting your actions. Customers using Google Cloud Platform retain all rights and respons bilities to configure and manage their environment, including configuring appropriate regions and zones to prevent failures or disasters. Customers must also secure their own data, and retain full responsibility for its protection.
O53-1	Customers are required to secure their user's biometrics data, when used.
O54	Google is certified to the ISO27001 Standard, which regulates "Capacity Management" (ISO 27001:2013, Annex A.12.1.3). Customers using Google Cloud Platform retain all rights and respons bilities to configure and manage their environment, including resource management.
O55	Google is certified to the ISO27001 Standard, which regulates "Communications Security" (ISO 27001:2013, Annex A.13), and "Securing Application Service on Public Networks" ISO 27001:2013, (Annex A.14.1.2). Customers using Google Cloud Platform retain all rights and respons bilities to configure and manage their environment, including management of external connections.
O56	Google is certified to the ISO27001 Standard, which regulates "Communications Security" (ISO 27001:2013, Annex A.13), and "Securing Application Service on Public Networks" (ISO 27001:2013, Annex A.14.1.2). Customers using Google Cloud Platform retain all rights and respons bilities to configure and manage their environment, including management of external connections.
O57	Google is certified to the ISO27001 Standard, which regulates "Equipment" (ISO 27001:2013, Annex A.11.2). Google's focus on security and protection of data is among our primary design criteria. Google data center physical security features a layered security model, including safeguards l ke custom-designed electronic access cards, alarms, vehicle access barriers, perimeter fencing, metal detectors, biometrics, and the data center floor features laser beam intrusion detection. Our data centers are monitored 24/7 by high-resolution interior and exterior cameras that can detect and track intruders. Access logs, activity records, and camera footage are available in case an incident occurs. Data centers are also routinely patrolled by experienced security guards who have undergone rigorous background checks and training. To learn more about our Data Center Processes, please see our Security Whitepaper and Data Center Introduction videos: Google Security Whitepaper: https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers
O58	Google is certified to the ISO27001 Standard, which regulates "Equipment" (ISO 27001:2013, Annex A.11.2). Google's focus on security and protection of data is among our primary design criteria. Google data center physical security features a layered security model, including safeguards l ke custom-designed electronic access cards, alarms, vehicle access barriers, perimeter fencing, metal detectors, biometrics, and the data center floor features laser beam intrusion detection. Our data centers are monitored 24/7 by high-resolution interior and exterior cameras that can detect and track intruders. Access logs, activity records, and camera footage are available in case an incident occurs. Data centers are also routinely patrolled by experienced security guards who have undergone rigorous background checks and training. To learn more about our Data Center Processes, please see our Security Whitepaper and Data Center Introduction videos: Google Security Whitepaper: https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers
O59	Google is certified to the ISO27001 Standard, which regulates "Equipment" (ISO 27001:2013, Annex A.11.2.4).
O60	Google is certified to the ISO27001 Standard, which regulates "Logging and Monitoring" (ISO 27001:2013, Annex A.12.4). Controls relating to availability and integrity of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google's security monitoring program is focused on information gathered from internal network traffic, employee actions on systems and outside knowledge of vulnerabilities. At many points across our global network, internal traffic is inspected for suspicious behavior, such as the presence of traffic that might indicate botnet connections. This analysis is performed using a combination of open-source and commercial tools for traffic capture and parsing. A proprietary correlation system built on top of Google technology also supports this analysis. Network analysis is supplemented by examining system logs to identify unusual behavior, such as attempted access of customer data. Google security engineers place standing search alerts on public data repositories to look for security incidents that might affect the company's infrastructure. They actively review inbound security reports and monitor public mailing lists, blog posts, and wikis. Automated network analysis helps determine when an unknown threat may exist and escalates to Google security staff, and network analysis is supplemented by automated analysis of system logs. Customers using Google Cloud Platform, retain all rights and responsibilities to configure and manage and monitor their environment.
O61	Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001:2013, Annex A.11). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Physical access to secured areas (such as the data server floor) is only possible via a security corridor. Google implements multi-factor access control using security badges and biometrics. Only approved employees with specific roles may enter secured areas, and all access to those area is monitored, logged and periodically approved for appropriateness. Employees with access must follow documented policies and procedures for the type of secured areas they are working in.
O62	Google is certified to the ISO27001 Standard, which regulates "Redundancies" (ISO27001:2013, Annex A.17.2) and "Backup" (ISO27001:2013 Annex A 12.3.) Controls relating to availability and integrity of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google designs the components of our platform to be highly redundant. This redundancy applies to our server design, how we store data, network and internet connectivity, and the software services themselves. This "redundancy of everything" includes the handling of errors by design and creates a solution that is not dependant on a single server, data center, or network connection. Google's data centers are geographically distr buted to minimize the effects of regional disruptions such as natural disasters and local outages. In the event of hardware, software, or network failure, data is automatically shifted from one facility to another so that Google Cloud and G Suite customers can continue working in most cases without interruption. Google's highly redundant infrastructure also helps protect our customers from data loss. For Google Cloud Products (G Suite and Google Cloud Platform), our Recovery Point Objective (RPO) target is zero, and our recovery time objective (RTO) design target is also zero. We aim to achieve these targets through live or synchronous replication: actions you take in Cloud products are simultaneously replicated in two data centers at once, so that if one data center fails, we transfer your data over to the other one that's also been reflecting your actions. Customers using Google Cloud Platform retain all rights and respons bilities to configure and manage their environment, including configuring appropriate regions and zones to prevent failures or disasters.
O63	Google is certified to the ISO27001 Standard, which regulates "Redundancies" (ISO27001:2013, Annex A.17.2) and "Backup" (ISO27001:2013 Annex A 12.3.) Controls relating to availability and integrity of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google designs the components of our platform to be highly redundant. This redundancy applies to our server design, how we store data, network and internet connectivity, and the software services themselves. This "redundancy of everything" includes the handling of errors by design and creates a solution that is not dependant on a single server, data center, or network connection. Google's data centers are geographically distr buted to minimize the effects of regional disruptions such as natural disasters and local outages. In the event of hardware, software, or network failure, data is automatically shifted from one facility to another so that Google Cloud and G Suite customers can continue working in most cases without interruption. Google's highly redundant infrastructure also helps protect our customers from data loss. For Google Cloud Products (G Suite and Google Cloud Platform), our Recovery Point Objective (RPO) target is zero, and our recovery time objective (RTO) design target is also zero. We aim to achieve these targets through live or synchronous replication: actions you take in Cloud products are simultaneously replicated in two data centers at once, so that if one data center fails, we transfer your data over to the other one that's also been reflecting your actions. Customers using Google Cloud Platform retain all rights and respons bilities to configure and manage their environment, including configuring appropriate regions and zones to prevent failures or disasters.

O64	Google is certified to the ISO27001 Standard, which regulates "Redundancies" (ISO27001:2013, Annex A.17.2) and "Backup" (ISO27001:2013 Annex A 12.3.) Controls relating to availability and integrity of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google designs the components of our platform to be highly redundant. This redundancy applies to our server design, how we store data, network and internet connectivity, and the software services themselves. This “redundancy of everything” includes the handling of errors by design and creates a solution that is not dependant on a single server, data center, or network connection. Google’s data centers are geographically distr buted to minimize the effects of regional disruptions such as natural disasters and local outages. In the event of hardware, software, or network failure, data is automatically shifted from one facility to another so that Google Cloud and G Suite customers can continue working in most cases without interruption. Google’s highly redundant infrastructure also helps protect our customers from data loss. For Google Cloud Products (G Suite and Google Cloud Platform), our Recovery Point Objective (RPO) target is zero, and our recovery time objective (RTO) design target is also zero. We aim to achieve these targets through live or synchronous replication: actions you take in Cloud products are simultaneously replicated in two data centers at once, so that if one data center fails, we transfer your data over to the other one that's also been reflecting your actions. Customers using Google Cloud Platform retain all rights and respons bilities to configure and manage their environment, including configuring appropriate regions and zones to prevent failures or disasters.
O65	Google is certified to the ISO27001 Standard, which regulates "Information Security Continuity" (ISO 27001:2013, Annex A.17.1). Google designs the components of our platform to be highly redundant. This redundancy applies to our server design, how we store data, network and internet connectivity, and the software services themselves. This “redundancy of everything” includes the handling of errors by design and creates a solution that is not dependant on a single server, data center, or network connection. Google’s data centers are geographically distributed to minimize the effects of regional disruptions such as natural disasters and local outages. In the event of hardware, software, or network failure, data is automatically shifted from one facility to another so that Google Cloud and G Suite customers can continue working in most cases without interruption. Google’s highly redundant infrastructure also helps protect our customers from data loss. For Google Cloud Products (G Suite and Google Cloud Platform), our Recovery Point Objective (RPO) target is zero, and our recovery time objective (RTO) design target is also zero. We aim to achieve these targets through live or synchronous replication: actions you take in Cloud products are simultaneously replicated in two data centers at once, so that if one data center fails, we transfer your data over to the other one that's also been reflecting your actions. Google also maintains a robust internal DR program, including development of appropriate contingency plans. Customers using Google Cloud Platform retain all rights and respons bilities to configure and manage their environment, including developing appropriate contingency plans.
O66	Google is certified to the ISO27001 Standard, which regulates "Respons bility for Assets" (Annex A.8.1), "Disposal of Media" (Annex A.8.3.2), "Secure Disposal or Reuse of Equipment" (Annex A.11.2.7) and "Control of Operational Software (Annex A.12.5.). Google meticulously tracks the location and status of all equipment within our data centers from acquisition to installation to retirement to destruction, via bar codes and asset tags. Metal detectors and video surveillance are implemented to help make sure no equipment leaves the data center floor without authorization. If a component fails to pass a performance test at any point during its lifecycle, it is removed from inventory and retired. When a hard drive is retired, authorized individuals verify that the disk is erased by writing 0's to the drive and performing multiple step verification process to ensure the drive contains no data. If the drive cannot be erased for any reason, it is stored securely until it can be physically destroyed. Physical destruction of disks is a multi stage process beginning with a crusher that deforms the drive, followed by a shredder that breaks the drive into small pieces, which are then recycled at a secure facility. Each data center adheres to a strict disposal policy and any variances are immediately addressed. Customers using Google Cloud Platform retain all rights and respons bilities to configure and manage their environment.
O67	Google is certified to the ISO27001 Standard, which regulates "Separation of Development, Testing, and Operational Environments" (ISO 27001:2013, Annex A.12.1.4), " and Security in Development and Support Processes" (ISO 27001:2013, Annex A.14.2). Customers using Google Cloud Platform retain all rights and respons bilities to configure and manage their environment.
O68	Google is certified to the ISO27001 Standard, which regulates "Separation of Development, Testing, and Operational Environments" (ISO 27001:2013, Annex A.12.1.4), " and Security in Development and Support Processes" (ISO 27001:2013, Annex A.14.2). Customers using Google Cloud Platform retain all rights and respons bilities to configure and manage their environment.
O69	Google is certified to the ISO27001 Standard, which regulates "Separation of Development, Testing, and Operational Environments" (ISO 27001:2013, Annex A.12.1.4), " and Security in Development and Support Processes" (ISO 27001:2013, Annex A.14.2). Customers using Google Cloud Platform retain all rights and respons bilities to configure and manage their environment.
O70	Google is certified to the ISO27001 Standard, which regulates "Information Security Policy" (ISO 27001:2013, Annex A.5), Organization of Information Security (ISO27001:2013, Annex A.6) and Operational Procedures and Responsibilities (ISO 27001:2013, Annex A 12.1) Information security oversight and management controls, including documentation of information security policies are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Customers using Google Cloud Platform retain all rights and respons bilities to configure and manage their environment, including management of system documents.
O71	Google is certified to the ISO27001 Standard, which regulates "Information Security Policy" (ISO 27001:2013, Annex A.5), Organization of Information Security (ISO27001:2013, Annex A.6) and Operational Procedures and Responsibilities (ISO 27001:2013, Annex A 12.1) Information security oversight and management controls, including documentation of information security policies are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Customers using Google Cloud Platform retain all rights and respons bilities to configure and manage their environment, including storage management procedures.
O72	"Google is certified to the ISO27001 Standard, which regulates "System Acquisition, Development and Maintenance" (ISO27001:2013, Annex A.14.2). Please see the Google Infrastructure Security Design Overview - https://cloud.google.com/security/security-design/ for more details. Customers using Google Cloud Platform retain all rights and respons bilities to configure and manage their environment, including system development procedures.
O73	Google is certified to the ISO27001 Standard, which regulates "System Acquisition, Development and Maintenance" (ISO27001:2013, Annex A.14.2). Please see the Google Infrastructure Security Design Overview - https://cloud.google.com/security/security-design/ for more details. Customers using Google Cloud Platform retain all rights and respons bilities to configure and manage their environment, including system development procedures.
O74	Google is certified to the ISO27001 Standard, which regulates "Disposal of Media" ((ISO 27001:2013, Annex A.8.3.2), "Secure disposal or reuse of equipment" ((ISO 27001:2013,Annex A.11.2.7). Google meticulously tracks the location and status of all equipment within our data centers from acquisition to installation to retirement to destruction, via bar codes and asset tags. Metal detectors and video surveillance are implemented to help make sure no equipment leaves the data center floor without authorization. If a component fails to pass a performance test at any point during its lifecycle, it is removed from inventory and retired. When a hard drive is retired, authorized individuals verify that the disk is erased by writing 0's to the drive and performing multiple step verification process to ensure the drive contains no data. If the drive cannot be erased for any reason, it is stored securely until it can be physically destroyed. Physical destruction of disks is a multi stage process beginning with a crusher that deforms the drive, followed by a shredder that breaks the drive into small pieces, which are then recycled at a secure facility. Each data center adheres to a strict disposal policy and any variances are immediately addressed.
O75	Google is certified to the ISO27001 Standard, which regulates "Disposal of Media" (ISO 27001:2013, Annex A.8.3.2), "Secure disposal or reuse of equipment" (ISO 27001:2013,Annex A.11.2.7). Google meticulously tracks the location and status of all equipment within our data centers from acquisition to installation to retirement to destruction, via bar codes and asset tags. Metal detectors and video surveillance are implemented to help make sure no equipment leaves the data center floor without authorization. If a component fails to pass a performance test at any point during its lifecycle, it is removed from inventory and retired. When a hard drive is retired, authorized individuals verify that the disk is erased by writing 0's to the drive and performing multiple step verification process to ensure the drive contains no data. If the drive cannot be erased for any reason, it is stored securely until it can be physically destroyed. Physical destruction of disks is a multi stage process beginning with a crusher that deforms the drive, followed by a shredder that breaks the drive into small pieces, which are then recycled at a secure facility. Each data center adheres to a strict disposal policy and any variances are immediately addressed.

O76	Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001:2013, Annex A.11). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google's focus on security and protection of data is among our primary design criteria. Google data center physical security features a layered security model, including safeguards l ke custom-designed electronic access cards, alarms, vehicle access barriers, perimeter fencing, metal detectors, biometrics, and the data center floor features laser beam intrusion detection. Our data centers are monitored 24/7 by high-resolution interior and exterior cameras that can detect and track intruders. Access logs, activity records, and camera footage are available in case an incident occurs. Data centers are also routinely patrolled by experienced security guards who have undergone rigorous background checks and training. To learn more about our Data Center Processes, please see our Security Whitepaper and Data Center Introduction videos: Google Security Whitepaper: https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers Data Center Introduction Video: https://www.youtube.com/watch?v=XZmGGAbHqa0
O77	Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001:2013, Annex A.11). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google's focus on security and protection of data is among our primary design criteria. Google data center physical security features a layered security model, including safeguards l ke custom-designed electronic access cards, alarms, vehicle access barriers, perimeter fencing, metal detectors, biometrics, and the data center floor features laser beam intrusion detection. Our data centers are monitored 24/7 by high-resolution interior and exterior cameras that can detect and track intruders. Access logs, activity records, and camera footage are available in case an incident occurs. Data centers are also routinely patrolled by experienced security guards who have undergone rigorous background checks and training. To learn more about our Data Center Processes, please see our Security Whitepaper and Data Center Introduction videos: Google Security Whitepaper: https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers Data Center Introduction Video: https://www.youtube.com/watch?v=XZmGGAbHqa0
O78	Google is certified to the ISO27001 Standard, which regulates "Capacity Management" (ISO 27001:2013, Annex A.12.1.3). Google has a robust network that monitors and adjusts capacity on an as-needed basis worldwide.
O79	Google is certified to the ISO27001 Standard, which regulates "Logging and Monitoring" (ISO 27001:2013, Annex A.12.4). Controls relating to availability and integrity of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google's security monitoring program is focused on information gathered from internal network traffic, employee actions on systems and outside knowledge of vulnerabilities. At many points across our global network, internal traffic is inspected for suspicious behavior, such as the presence of traffic that might indicate botnet connections. This analysis is performed using a combination of open-source and commercial tools for traffic capture and parsing. A proprietary correlation system built on top of Google technology also supports this analysis. Network analysis is supplemented by examining system logs to identify unusual behavior, such as attempted access of customer data. Google security engineers place standing search alerts on public data repositories to look for security incidents that might affect the company's infrastructure. They actively review inbound security reports and monitor public mailing lists, blog posts, and wikis. Automated network analysis helps determine when an unknown threat may exist and escalates to Google security staff, and network analysis is supplemented by automated analysis of system logs.
O80	Google is certified to the ISO27001 Standard, which regulates "Information Security Awareness, Education and Training" (ISO 27001:2013, Annex A.7.2.2), Information security oversight and management controls, including management of security awareness and training are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. All Google contractors undergo security training as part of the orientation process and receive ongoing security training throughout their Google careers. During orientation, new contractors agree to our Code of Conduct, which highlights our commitment to keep customer information safe and secure. Depending on their job role, additional training on specific aspects of security may be required. For instance, the information security team instructs new engineers on topics l ke secure coding practices, product design and automated vulnerability testing tools. Engineers also attend technical presentations on security-related topics and receive a security newsletter that covers new threats, attack patterns, mitigation techniques and more.
O81	Google is certified to the ISO27001 Standard, which regulates "Information Security Awareness, Education and Training" (ISO 27001:2013, Annex A.7.2.2), Information security oversight and management controls, including management of security awareness and training are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. All Google contractors undergo security training as part of the orientation process and receive ongoing security training throughout their Google careers. During orientation, new contractors agree to our Code of Conduct, which highlights our commitment to keep customer information safe and secure. Depending on their job role, additional training on specific aspects of security may be required. For instance, the information security team instructs new engineers on topics l ke secure coding practices, product design and automated vulnerability testing tools. Engineers also attend technical presentations on security-related topics and receive a security newsletter that covers new threats, attack patterns, mitigation techniques and more.
O82	Google is certified to the ISO27001 Standard, which regulates "Information Security Awareness, Education and Training" (ISO 27001:2013, Annex A.7.2.2), Information security oversight and management controls, including management of security awareness and training are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. All Google contractors undergo security training as part of the orientation process and receive ongoing security training throughout their Google careers. During orientation, new contractors agree to our Code of Conduct, which highlights our commitment to keep customer information safe and secure. Depending on their job role, additional training on specific aspects of security may be required. For instance, the information security team instructs new engineers on topics l ke secure coding practices, product design and automated vulnerability testing tools. Engineers also attend technical presentations on security-related topics and receive a security newsletter that covers new threats, attack patterns, mitigation techniques and more.
O83	Google is certified to the ISO27001 Standard, which regulates "Information Security Awareness, Education and Training" (ISO 27001:2013, Annex A.7.2.2), Information security oversight and management controls, including management of security awareness and training are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. All Google contractors undergo security training as part of the orientation process and receive ongoing security training throughout their Google careers. During orientation, new contractors agree to our Code of Conduct, which highlights our commitment to keep customer information safe and secure. Depending on their job role, additional training on specific aspects of security may be required. For instance, the information security team instructs new engineers on topics l ke secure coding practices, product design and automated vulnerability testing tools. Engineers also attend technical presentations on security-related topics and receive a security newsletter that covers new threats, attack patterns, mitigation techniques and more.
O84	Google is certified to the ISO27001 Standard, which regulates "Information Security Awareness, Education and Training" (ISO 27001:2013, Annex A.7.2.2), Information security oversight and management controls, including management of security awareness and training are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. All Google contractors undergo security training as part of the orientation process and receive ongoing security training throughout their Google careers. During orientation, new contractors agree to our Code of Conduct, which highlights our commitment to keep customer information safe and secure. Depending on their job role, additional training on specific aspects of security may be required. For instance, the information security team instructs new engineers on topics l ke secure coding practices, product design and automated vulnerability testing tools. Engineers also attend technical presentations on security-related topics and receive a security newsletter that covers new threats, attack patterns, mitigation techniques and more.
O85	Google is certified to the ISO27001 Standard, which regulates "Human Resources Security" (ISO27001:2013, Annex A.7). Controls relating to human resource management are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Customers using Google Cloud Platform retain all rights and respons bilities to configure and manage their environment, including human resource management.
O86	Google is certified to the ISO27001 Standard, which regulates "Human Resources Security" (ISO27001:2013, Annex A.7). Controls relating to human resource management are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Customers using Google Cloud Platform retain all rights and respons bilities to configure and manage their environment, including human resource management.

O87	Google is certified to the ISO27001 Standard, which regulates "Supplier Relationships" (ISO 27001:2013, Annex A.15). Information security oversight and management controls, including vendor security practices are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google directly conducts virtually all data processing activities to provide our services. However, Google may engage some third-party suppliers to provide services, including customer and technical support. Prior to onboarding third-party suppliers, Google conducts an assessment of the security and privacy practices of third-party suppliers to ensure they provide a level of security and privacy appropriate to their access to data and the scope of the services they are engaged to provide. Once Google has assessed the risks presented by the third-party supplier, the supplier is required to enter into appropriate security, confidentiality, and privacy contract terms. https://cloud.google.com/terms/subprocessors https://G Suite.google.com/terms/subprocessors.html
O87-1	Google is certified to the ISO27001 Standard, which regulates "Supplier Relationships" (ISO 27001:2013, Annex A.15). Information security oversight and management controls, including vendor security practices are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google directly conducts virtually all data processing activities to provide our services. However, Google may engage some third-party suppliers to provide services, including customer and technical support. Prior to onboarding third-party suppliers, Google conducts an assessment of the security and privacy practices of third-party suppliers to ensure they provide a level of security and privacy appropriate to their access to data and the scope of the services they are engaged to provide. Once Google has assessed the risks presented by the third-party supplier, the supplier is required to enter into appropriate security, confidentiality, and privacy contract terms. https://cloud.google.com/terms/subprocessors https://G Suite.google.com/terms/subprocessors.html
O88	Google is certified to the ISO27001 Standard, which regulates "Supplier Relationships" (ISO 27001:2013, Annex A.15). Information security oversight and management controls, including vendor security practices are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google directly conducts virtually all data processing activities to provide our services. However, Google may engage some third-party suppliers to provide services, including customer and technical support. Prior to onboarding third-party suppliers, Google conducts an assessment of the security and privacy practices of third-party suppliers to ensure they provide a level of security and privacy appropriate to their access to data and the scope of the services they are engaged to provide. Once Google has assessed the risks presented by the third-party supplier, the supplier is required to enter into appropriate security, confidentiality, and privacy contract terms. https://cloud.google.com/terms/subprocessors https://G Suite.google.com/terms/subprocessors.html
O89	Google is certified to the ISO27001 Standard, which regulates "Information Security Awareness, Education and Training" (ISO 27001:2013, Annex A.7.2.2), Information security oversight and management controls, including management of security awareness and training are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. All Google contractors undergo security training as part of the orientation process and receive ongoing security training throughout their Google careers. During orientation, new contractors agree to our Code of Conduct, which highlights our commitment to keep customer information safe and secure. Depending on their job role, additional training on specific aspects of security may be required. For instance, the information security team instructs new engineers on topics l ke secure coding practices, product design and automated vulnerability testing tools. Engineers also attend technical presentations on security-related topics and receive a security newsletter that covers new threats, attack patterns, mitigation techniques and more.
O90	Google is certified to the ISO27001 Standard, which regulates "Supplier Relationships" (ISO 27001:2013, Annex A.15). Information security oversight and management controls, including vendor security practices are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google directly conducts virtually all data processing activities to provide our services. However, Google may engage some third-party suppliers to provide services related to Cloud Platform, including customer and technical support. Prior to onboarding third-party suppliers, Google conducts an assessment of the security and privacy practices of third-party suppliers to ensure they provide a level of security and privacy appropriate to their access to data and the scope of the services they are engaged to provide. Once Google has assessed the risks presented by the third-party supplier, the supplier is required to enter into appropriate security, confidentiality, and privacy contract terms.
O90-1	Google does not maintain financial transaction software for customers. The responsibility of maintaining CD/ATM networks remains with the customer.
O91	Google is certified to the ISO27001 Standard, which regulates "Information Systems Audit Considerations" (ISO 27001:2013, Annex A.12.7), Information security oversight and management controls, including the establishment of internal audit oversight are reviewed and verified by a third party auditor for Google's SOC 2, Type II report
O92	Responsibility for in-store branches rests with the customer and it out of scope for Google's platform.
O93	Responsibility for ATMs in convenience stores rests with the customer and is out of scope for Google's platform.
O94	Responsibility for ATMs in convenience stores rests with the customer and is out of scope for Google's platform.
O95	Responsibility for ATMs in convenience stores rests with the customer and is out of scope for Google's platform.
O96	Responsibility for ATMs in convenience stores rests with the customer and is out of scope for Google's platform.
O97	Responsibility for ATMs in convenience stores rests with the customer and is out of scope for Google's platform.
O98	Responsibility for ATMs in convenience stores rests with the customer and is out of scope for Google's platform.
O99	Responsibility for debit cards rests with the customer and is out of scope for Google's platform.
O100	Responsibility for debit cards rests with the customer and is out of scope for Google's platform.
O101	Responsibility for debit cards rests with the customer and is out of scope for Google's platform.
O102	Responsibility for debit cards rests with the customer and is out of scope for Google's platform.
O103	Responsibility for financial services using open networks rests with the customer and is out of scope for Google's platform.
O104	Responsibility for financial services using open networks rests with the customer and is out of scope for Google's platform.
O105	Responsibility for financial services using open networks rests with the customer and is out of scope for Google's platform.
O105-1	Responsibility for financial services using open networks rests with the customer and is out of scope for Google's platform.
O106	Responsibility for financial services using open networks rests with the customer and is out of scope for Google's platform.
O107	Responsibility for financial services using open networks rests with the customer and is out of scope for Google's platform.
O108	Due diligence in selection of a cloud provider is an end-user responsibility. Google provides public-facing information regarding its offerings to allow potential customers to evaluate specific products.
O109	Google Cloud and G Suite are certified to the ISO27017 standard for cloud providers. Please see Google's Terms of Service and SLA guidance, which outline contractual obligations and agreements. Terms of Service: https://cloud.google.com/terms/ https://G Suite.google.com/terms/2013/1/premier_terms.html SLA: https://G Suite.google.com/terms/sla.html https://cloud.google.com/terms/sla/
O110	Google is certified to the ISO27001 Standard, which regulates "Cryptography" (ISO 27001:2013, Annex A.10) Google publishes details about encryption and key management options for its Google Cloud and G Suite products. To read more about key management and encryption, please see: https://cloud.google.com/security/encryption-at-rest/ https://storage.googleapis.com/gfw-touched-accounts-pdfs/google-encryption-whitepaper-G Suite.pdf Customers using Google Cloud Platform retain all rights and respons bilities to configure and manage their environment, including development of appropriate encryption measures.
O111	Cloud Platform customers own their data, not Google. The data that customers put into our systems is theirs, and we do not scan it for advertisements nor sell it to third parties. We offer our customers a detailed data processing amendment that describes our commitment to protecting customer data. It states that Google will not process data for any purpose other than to fulfill our contractual obligations. Furthermore, if customers delete their data, we commit to deleting it from our systems within 180 days. Finally, we provide tools that make it easy for customers to take their data with them if they choose to stop using our services, without penalty or additional cost imposed by Google. Customers using Google Cloud Platform retain all rights and respons bilities to configure and manage their environment, including development of appropriate encryption measures.

O112	Google is certified to the ISO27001 Standard, which regulates "Independent Review of Information Security" (ISO 27001:2013, Annex A.18.2.1). In addition, Google Cloud and G Suite are certified to the ISO27017 standard for cloud providers. Google conducts a number of audits to provide 3rd party validation of our control environment and provides validation of audits to customers, as needed. To review our current list of 3rd party compliance audits, please see the following pages: https://cloud.google.com/security/compliance https://G Suite.google.com/learn-more/compliance-google-apps.html
O113	Google is certified to the ISO27001 Standard, which regulates "Protection from Malware" ISO 27001:2013, (Annex A.12.2). Controls relating to vulnerability management are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google administers a vulnerability management process that actively scans for security threats using a combination of commercially available and purpose-built in house tools, intensive automated and manual penetration efforts, quality assurance processes, software security reviews and external audits. The vulnerability management team is respons ble for tracking and following up on vulnerabilities. Once a vulnerability requiring remediation has been identified, it is logged, prioritized according to severity, and assigned an owner. The vulnerability management team tracks such issues and follows up frequently until they can verify that the issues have been remediated. Google also maintains relationships and interfaces with members of the security research community to track reported issues in Google services and open source tools. More information about reporting security issues can be found at www.google.com/intl/en/corporate/security.html.
Technical	
Item No.	**Google Response**
T1	Google is certified to the ISO27001 Standard, which regulates "Equipment Maintenance" (Annex A.11.2.4). Google's infrastructure utilizes container technology, and handles device failures flex ble and seamlessly. It monitors malfunctioning devices constantly, and continues service even when problems are detected by transmitting data to other devices.
T2	Google is certified to the ISO27001 Standard, which regulates "Redundancies" (ISO27001:2013, Annex A.17.2). Controls relating to availability and integrity of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google designs the components of our platform to be highly redundant. This redundancy applies to our server design, how we store data, network and internet connectivity, and the software services themselves. This "redundancy of everything" includes the handling of errors by design and creates a solution that is not dependant on a single server, data center, or network connection. Google's data centers are geographically distributed to minimize the effects of regional disruptions such as natural disasters and local outages. In the event of hardware, software, or network failure, data is automatically shifted from one facility to another so that Google Cloud and G Suite customers can continue working in most cases without interruption. Google's highly redundant infrastructure also helps protect our customers from data loss. For Google Cloud Products (G Suite and Google Cloud Platform), our Recovery Point Objective (RPO) target is zero, and our recovery time objective (RTO) design target is also zero. We aim to achieve these targets through live or synchronous replication: actions you take in Cloud products are simultaneously replicated in two data centers at once, so that if one data center fails, we transfer your data over to the other one that's also been reflecting your actions. Customers using Google Cloud Platform retain all rights and respons bilities to configure and manage their environment, including configuring appropriate regions and zones to prevent failures or disasters.
T3	Google is certified to the ISO27001 Standard, which regulates "Redundancies" (ISO27001:2013, Annex A.17.2). Controls relating to availability and integrity of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google designs the components of our platform to be highly redundant. This redundancy applies to our server design, how we store data, network and internet connectivity, and the software services themselves. This "redundancy of everything" includes the handling of errors by design and creates a solution that is not dependant on a single server, data center, or network connection. Google's data centers are geographically distributed to minimize the effects of regional disruptions such as natural disasters and local outages. In the event of hardware, software, or network failure, data is automatically shifted from one facility to another so that Google Cloud and G Suite customers can continue working in most cases without interruption. Google's highly redundant infrastructure also helps protect our customers from data loss. For Google Cloud Products (G Suite and Google Cloud Platform), our Recovery Point Objective (RPO) target is zero, and our recovery time objective (RTO) design target is also zero. We aim to achieve these targets through live or synchronous replication: actions you take in Cloud products are simultaneously replicated in two data centers at once, so that if one data center fails, we transfer your data over to the other one that's also been reflecting your actions. Customers using Google Cloud Platform retain all rights and respons bilities to configure and manage their environment, including configuring appropriate regions and zones to prevent failures or disasters.
T4	Google is certified to the ISO27001 Standard, which regulates "Redundancies" (ISO27001:2013, Annex A.17.2). Controls relating to availability and integrity of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google designs the components of our platform to be highly redundant. This redundancy applies to our server design, how we store data, network and internet connectivity, and the software services themselves. This "redundancy of everything" includes the handling of errors by design and creates a solution that is not dependant on a single server, data center, or network connection. Google's data centers are geographically distributed to minimize the effects of regional disruptions such as natural disasters and local outages. In the event of hardware, software, or network failure, data is automatically shifted from one facility to another so that Google Cloud and G Suite customers can continue working in most cases without interruption. Google's highly redundant infrastructure also helps protect our customers from data loss. For Google Cloud Products (G Suite and Google Cloud Platform), our Recovery Point Objective (RPO) target is zero, and our recovery time objective (RTO) design target is also zero. We aim to achieve these targets through live or synchronous replication: actions you take in Cloud products are simultaneously replicated in two data centers at once, so that if one data center fails, we transfer your data over to the other one that's also been reflecting your actions. Customers using Google Cloud Platform retain all rights and respons bilities to configure and manage their environment, including configuring appropriate regions and zones to prevent failures or disasters.
T5	Google is certified to the ISO27001 Standard, which regulates "Redundancies" (ISO27001:2013, Annex A.17.2). Controls relating to availability and integrity of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google designs the components of our platform to be highly redundant. This redundancy applies to our server design, how we store data, network and internet connectivity, and the software services themselves. This "redundancy of everything" includes the handling of errors by design and creates a solution that is not dependant on a single server, data center, or network connection. Google's data centers are geographically distributed to minimize the effects of regional disruptions such as natural disasters and local outages. In the event of hardware, software, or network failure, data is automatically shifted from one facility to another so that Google Cloud and G Suite customers can continue working in most cases without interruption. Google's highly redundant infrastructure also helps protect our customers from data loss. For Google Cloud Products (G Suite and Google Cloud Platform), our Recovery Point Objective (RPO) target is zero, and our recovery time objective (RTO) design target is also zero. We aim to achieve these targets through live or synchronous replication: actions you take in Cloud products are simultaneously replicated in two data centers at once, so that if one data center fails, we transfer your data over to the other one that's also been reflecting your actions. Customers using Google Cloud Platform retain all rights and respons bilities to configure and manage their environment, including configuring appropriate regions and zones to prevent failures or disasters.
T6	Google is certified to the ISO27001 Standard, which regulates "Redundancies" (ISO27001:2013, Annex A.17.2). Controls relating to availability and integrity of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google designs the components of our platform to be highly redundant. This redundancy applies to our server design, how we store data, network and internet connectivity, and the software services themselves. This "redundancy of everything" includes the handling of errors by design and creates a solution that is not dependant on a single server, data center, or network connection. Google's data centers are geographically distributed to minimize the effects of regional disruptions such as natural disasters and local outages. In the event of hardware, software, or network failure, data is automatically shifted from one facility to another so that Google Cloud and G Suite customers can continue working in most cases without interruption. Google's highly redundant infrastructure also helps protect our customers from data loss. For Google Cloud Products (G Suite and Google Cloud Platform), our Recovery Point Objective (RPO) target is zero, and our recovery time objective (RTO) design target is also zero. We aim to achieve these targets through live or synchronous replication: actions you take in Cloud products are simultaneously replicated in two data centers at once, so that if one data center fails, we transfer your data over to the other one that's also been reflecting your actions. Customers using Google Cloud Platform retain all rights and respons bilities to configure and manage their environment, including configuring appropriate regions and zones to prevent failures or disasters.
T7	Google is certified to the ISO27001 Standard, which regulates "System Acquisition, Development and Maintenance" (ISO27001:2013, Annex A.14.2). Customers using Google Cloud Platform retain all rights and respons bilities to configure and manage their environment, including managing their system development process.
T8	Google is certified to the ISO27001 Standard, which regulates "System Acquisition, Development and Maintenance" (ISO27001:2013, Annex A.14.2). Customers using Google Cloud Platform retain all rights and respons bilities to configure and manage their environment, including managing their system development process.

T9	Google is certified to the ISO27001 Standard, which regulates "System Acquisition, Development and Maintenance" (ISO27001:2013, Annex A.14.2). Customers using Google Cloud Platform retain all rights and respons bilities to configure and manage their environment, including managing their system development process.
T10	Google is certified to the ISO27001 Standard, which regulates "System Acquisition, Development and Maintenance" (ISO27001:2013, Annex A.14.2). Customers using Google Cloud Platform retain all rights and respons bilities to configure and manage their environment, including managing their system development process.
T11	Google is certified to the ISO27001 Standard, which regulates "System Acquisition, Development and Maintenance" (ISO27001:2013, Annex A.14.2). Customers using Google Cloud Platform retain all rights and respons bilities to configure and manage their environment, including managing their system development process.
T12	Google is certified to the ISO27001 Standard, which regulates "System Acquisition, Development and Maintenance" (ISO27001:2013, Annex A.14.2). Customers using Google Cloud Platform retain all rights and respons bilities to configure and manage their environment, including managing their system development process.
T13	Google is certified to the ISO27001 Standard, which regulates "System Acquisition, Development and Maintenance" (ISO27001:2013, Annex A.14.2). Customers using Google Cloud Platform retain all rights and respons bilities to configure and manage their environment, including managing their system development process.
T14	Google is certified to the ISO27001 Standard, which regulates "Change Management" (ISO27001:2013 Annex A 12.1.2) and "System Acquisition, Development and Maintenance" (ISO27001:2013, Annex A.14.2). Please see the Google Infrastructure Security Design Overview - https://cloud.google.com/security/security-design/ for more details. Customers using Google Cloud Platform retain all rights and respons bilities to configure and manage their environment, including change management and system development procedures.
T15	Google is certified to the ISO27001 Standard, which regulates "Change Management" (ISO27001:2013 Annex A 12.1.2) and "System Acquisition, Development and Maintenance" (ISO27001:2013, Annex A.14.2). Please see the Google Infrastructure Security Design Overview - https://cloud.google.com/security/security-design/ for more details. Customers using Google Cloud Platform retain all rights and respons bilities to configure and manage their environment, including change management and system development procedures.
T16	Google is certified to the ISO27001 Standard, which regulates "System Acquisition, Development and Maintenance" (ISO27001:2013, Annex A.14.2). Please see the Google Infrastructure Security Design Overview - https://cloud.google.com/security/security-design/ for more details. Customers using Google Cloud Platform retain all rights and respons bilities to configure and manage their environment, including system development procedures.
T17	Google is certified to the ISO27001 Standard, which regulates "System Acquisition, Development and Maintenance" (ISO27001:2013, Annex A.14.2). Please see the Google Infrastructure Security Design Overview - https://cloud.google.com/security/security-design/ for more details. Customers using Google Cloud Platform retain all rights and respons bilities to configure and manage their environment, including system development procedures.
T18	Google is certified to the ISO27001 Standard, which regulates "System Acquisition, Development and Maintenance" (ISO27001:2013, Annex A.14.2). Please see the Google Infrastructure Security Design Overview - https://cloud.google.com/security/security-design/ for more details. Customers using Google Cloud Platform retain all rights and respons bilities to configure and manage their environment, including system development procedures.
T19	Responsibility for validation of remote control functions for CD/ATM rests with the customer.
T20	Google is certified to the ISO27001 Standard, which regulates "Logging and Monitoring" (ISO 27001:2013, Annex A.12.4). Controls relating to availability and integrity of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google’s security monitoring program is focused on information gathered from internal network traffic, employee actions on systems and outside knowledge of vulnerabilities. At many points across our global network, internal traffic is inspected for suspicious behavior, such as the presence of traffic that might indicate botnet connections. This analysis is performed using a combination of open-source and commercial tools for traffic capture and parsing. A proprietary correlation system built on top of Google technology also supports this analysis. Network analysis is supplemented by examining system logs to identify unusual behavior, such as attempted access of customer data. Google security engineers place standing search alerts on public data repositories to look for security incidents that might affect the company’s infrastructure. They actively review inbound security reports and monitor public mailing lists, blog posts, and wikis. Automated network analysis helps determine when an unknown threat may exist and escalates to Google security staff, and network analysis is supplemented by automated analysis of system logs.
T21	Google is certified to the ISO27001 Standard, which regulates "Logging and Monitoring" (ISO 27001:2013, Annex A.12.4). Controls relating to availability and integrity of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google’s security monitoring program is focused on information gathered from internal network traffic, employee actions on systems and outside knowledge of vulnerabilities. At many points across our global network, internal traffic is inspected for suspicious behavior, such as the presence of traffic that might indicate botnet connections. This analysis is performed using a combination of open-source and commercial tools for traffic capture and parsing. A proprietary correlation system built on top of Google technology also supports this analysis. Network analysis is supplemented by examining system logs to identify unusual behavior, such as attempted access of customer data. Google security engineers place standing search alerts on public data repositories to look for security incidents that might affect the company’s infrastructure. They actively review inbound security reports and monitor public mailing lists, blog posts, and wikis. Automated network analysis helps determine when an unknown threat may exist and escalates to Google security staff, and network analysis is supplemented by automated analysis of system logs.
T22	Google is certified to the ISO27001 Standard, which regulates "Logging and Monitoring" (ISO 27001:2013, Annex A.12.4). Controls relating to availability and integrity of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google’s security monitoring program is focused on information gathered from internal network traffic, employee actions on systems and outside knowledge of vulnerabilities. At many points across our global network, internal traffic is inspected for suspicious behavior, such as the presence of traffic that might indicate botnet connections. This analysis is performed using a combination of open-source and commercial tools for traffic capture and parsing. A proprietary correlation system built on top of Google technology also supports this analysis. Network analysis is supplemented by examining system logs to identify unusual behavior, such as attempted access of customer data. Google security engineers place standing search alerts on public data repositories to look for security incidents that might affect the company’s infrastructure. They actively review inbound security reports and monitor public mailing lists, blog posts, and wikis. Automated network analysis helps determine when an unknown threat may exist and escalates to Google security staff, and network analysis is supplemented by automated analysis of system logs.
T23	Responsibility for minimizing errors at the account level is the responsibility of the customer.
T24	Google is certified to the ISO27001 Standard, which regulates "Redundancies" (ISO27001:2013, Annex A.17.2). Controls relating to availability and integrity of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google designs the components of our platform to be highly redundant. This redundancy applies to our server design, how we store data, network and internet connectivity, and the software services themselves. This “redundancy of everything” includes the handling of errors by design and creates a solution that is not dependant on a single server, data center, or network connection. Google’s data centers are geographically distributed to minimize the effects of regional disruptions such as natural disasters and local outages. In the event of hardware, software, or network failure, data is automatically shifted from one facility to another so that Google Cloud and G Suite customers can continue working in most cases without interruption. Google’s highly redundant infrastructure also helps protect our customers from data loss. For Google Cloud Products (G Suite and Google Cloud Platform), our Recovery Point Objective (RPO) target is zero, and our recovery time objective (RTO) design target is also zero. We aim to achieve these targets through live or synchronous replication: actions you take in Cloud products are simultaneously replicated in two data centers at once, so that if one data center fails, we transfer your data over to the other one that's also been reflecting your actions.

T25	Google is certified to the ISO27001 Standard, which regulates "Redundancies" (ISO27001:2013, Annex A.17.2). Controls relating to availability and integrity of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google designs the components of our platform to be highly redundant. This redundancy applies to our server design, how we store data, network and internet connectivity, and the software services themselves. This “redundancy of everything” includes the handling of errors by design and creates a solution that is not dependant on a single server, data center, or network connection. Google’s data centers are geographically distributed to minimize the effects of regional disruptions such as natural disasters and local outages. In the event of hardware, software, or network failure, data is automatically shifted from one facility to another so that Google Cloud and G Suite customers can continue working in most cases without interruption. Google’s highly redundant infrastructure also helps protect our customers from data loss. For Google Cloud Products (G Suite and Google Cloud Platform), our Recovery Point Objective (RPO) target is zero, and our recovery time objective (RTO) design target is also zero. We aim to achieve these targets through live or synchronous replication: actions you take in Cloud products are simultaneously replicated in two data centers at once, so that if one data center fails, we transfer your data over to the other one that's also been reflecting your actions.
T26	Google is certified to the ISO27001 Standard, which regulates "Access Control" (ISO 27001:2013, Annex A.9). Information security oversight and management controls, including logical access controls are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. For Google employees, access rights and levels are based on an their job function and role, using the concepts of least–privilege and need–to–know to match access privileges to defined respons bilities. Google employees are only granted a limited set of default permissions to access company resources, such as employee email and Google’s internal employee portal. Requests for additional access follow a formal process that involves a request and an approval from a data or system owner, manager, or other executives, as dictated by Google’s security policies. Approvals are managed by workflow tools that maintain audit records of all changes. These tools control both the modification of authorization settings and the approval process to ensure consistent application of the approval policies. An employee’s authorization settings are used to control access to all resources, including data and systems for Google Cloud and G Suite products. Support services are only provided to authorized customer administrators whose identities have been verified in several ways. Googler access is monitored and audited by our dedicated security, privacy, and internal audit teams. Customers using Google Cloud Platform retain all rights and respons bilities to configure and manage their environment.
T27	Google is certified to the ISO27001 Standard, which regulates "Access Control" (ISO 27001:2013, Annex A.9). Information security oversight and management controls, including logical access controls are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. For Google employees, access rights and levels are based on an their job function and role, using the concepts of least–privilege and need–to–know to match access privileges to defined respons bilities. Google employees are only granted a limited set of default permissions to access company resources, such as employee email and Google’s internal employee portal. Requests for additional access follow a formal process that involves a request and an approval from a data or system owner, manager, or other executives, as dictated by Google’s security policies. Approvals are managed by workflow tools that maintain audit records of all changes. These tools control both the modification of authorization settings and the approval process to ensure consistent application of the approval policies. An employee’s authorization settings are used to control access to all resources, including data and systems for Google Cloud and G Suite products. Support services are only provided to authorized customer administrators whose identities have been verified in several ways. Googler access is monitored and audited by our dedicated security, privacy, and internal audit teams. Customers using Google Cloud Platform retain all rights and respons bilities to configure and manage their environment.
T28	Google is certified to the ISO27001 Standard, which regulates "Cryptography" (ISO 27001:2013, Annex A.10) Google publishes details about encryption and key management options for its Google Cloud and G Suite products. To read more about key management and encryption, please see: https://cloud.google.com/security/encryption-at-rest/ https://storage.googleapis.com/gfw-touched-accounts-pdfs/google-encryption-whitepaper-G Suite.pdf Customers using Google Cloud Platform retain all rights and respons bilities to configure and manage their environment, including development of appropriate encryption measures.
T29	Google is certified to the ISO27001 Standard, which regulates "Cryptography" (ISO 27001:2013, Annex A.10) Google publishes details about encryption and key management options for its Google Cloud and G Suite products. To read more about key management and encryption, please see: https://cloud.google.com/security/encryption-at-rest/ https://storage.googleapis.com/gfw-touched-accounts-pdfs/google-encryption-whitepaper-G Suite.pdf Customers using Google Cloud Platform retain all rights and respons bilities to configure and manage their environment, including development of appropriate encryption measures.
T30	Google is certified to the ISO27001 Standard, which regulates "System Acquisition, Development and Maintenance" (ISO27001:2013, Annex A.14.2). Please see the Google Infrastructure Security Design Overview - https://cloud.google.com/security/security-design/ for more details. Customers using Google Cloud Platform retain all rights and respons bilities to configure and manage their environment, including system development procedures.
T31	Google is certified to the ISO27001 Standard, which regulates "System Acquisition, Development and Maintenance" (ISO27001:2013, Annex A.14.2). Please see the Google Infrastructure Security Design Overview - https://cloud.google.com/security/security-design/ for more details. Customers using Google Cloud Platform retain all rights and respons bilities to configure and manage their environment, including system development procedures.
T32	Google is certified to the ISO27001 Standard, which regulates "System Acquisition, Development and Maintenance" (ISO27001:2013, Annex A.14.2). Please see the Google Infrastructure Security Design Overview - https://cloud.google.com/security/security-design/ for more details. Customers using Google Cloud Platform retain all rights and respons bilities to configure and manage their environment, including system development procedures.
T33	Google is certified to the ISO27001 Standard, which regulates "Logging and Monitoring" (ISO 27001:2013, Annex A.12.4). Controls relating to availability and integrity of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google’s security monitoring program is focused on information gathered from internal network traffic, employee actions on systems and outside knowledge of vulnerabilities. At many points across our global network, internal traffic is inspected for suspicious behavior, such as the presence of traffic that might indicate botnet connections. This analysis is performed using a combination of open-source and commercial tools for traffic capture and parsing. A proprietary correlation system built on top of Google technology also supports this analysis. Network analysis is supplemented by examining system logs to identify unusual behavior, such as attempted access of customer data. Google security engineers place standing search alerts on public data repositories to look for security incidents that might affect the company’s infrastructure. They actively review inbound security reports and monitor public mailing lists, blog posts, and wikis. Automated network analysis helps determine when an unknown threat may exist and escalates to Google security staff, and network analysis is supplemented by automated analysis of system logs. Customers using Google Cloud Platform retain all rights and respons bilities to configure and manage their environment, including configuration of specific monitoring to detect false or unverified data.
T34	Google is certified to the ISO27001 Standard, which regulates "Logging and Monitoring" (ISO 27001:2013, Annex A.12.4). Controls relating to availability and integrity of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google’s security monitoring program is focused on information gathered from internal network traffic, employee actions on systems and outside knowledge of vulnerabilities. At many points across our global network, internal traffic is inspected for suspicious behavior, such as the presence of traffic that might indicate botnet connections. This analysis is performed using a combination of open-source and commercial tools for traffic capture and parsing. A proprietary correlation system built on top of Google technology also supports this analysis. Network analysis is supplemented by examining system logs to identify unusual behavior, such as attempted access of customer data. Google security engineers place standing search alerts on public data repositories to look for security incidents that might affect the company’s infrastructure. They actively review inbound security reports and monitor public mailing lists, blog posts, and wikis. Automated network analysis helps determine when an unknown threat may exist and escalates to Google security staff, and network analysis is supplemented by automated analysis of system logs. Customers using Google Cloud Platform retain all rights and respons bilities to configure and manage their environment, including configuration of specific monitoring to detect false or unverified data.

T35	Google is certified to the ISO27001 Standard, which regulates "Access Control" (ISO 27001:2013, Annex A.9). Information security oversight and management controls, including logical access controls are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. For Google employees, access rights and levels are based on an their job function and role, using the concepts of least–privilege and need–to–know to match access privileges to defined respons bilities. Google employees are only granted a limited set of default permissions to access company resources, such as employee email and Google's internal employee portal. Requests for additional access follow a formal process that involves a request and an approval from a data or system owner, manager, or other executives, as dictated by Google's security policies. Approvals are managed by workflow tools that maintain audit records of all changes. These tools control both the modification of authorization settings and the approval process to ensure consistent application of the approval policies. An employee's authorization settings are used to control access to all resources, including data and systems for Google Cloud and G Suite products. Support services are only provided to authorized customer administrators whose identities have been verified in several ways. Googler access is monitored and audited by our dedicated security, privacy, and internal audit teams. Customers using Google Cloud Platform retain all rights and respons bilities to configure and manage their environment.
T35-1	Google is certified to the ISO27001 Standard, which regulates "Access Control" (ISO 27001:2013, Annex A.9). Information security oversight and management controls, including logical access controls are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. For Google employees, access rights and levels are based on an their job function and role, using the concepts of least–privilege and need–to–know to match access privileges to defined respons bilities. Google employees are only granted a limited set of default permissions to access company resources, such as employee email and Google's internal employee portal. Requests for additional access follow a formal process that involves a request and an approval from a data or system owner, manager, or other executives, as dictated by Google's security policies. Approvals are managed by workflow tools that maintain audit records of all changes. These tools control both the modification of authorization settings and the approval process to ensure consistent application of the approval policies. An employee's authorization settings are used to control access to all resources, including data and systems for Google Cloud and G Suite products. Support services are only provided to authorized customer administrators whose identities have been verified in several ways. Googler access is monitored and audited by our dedicated security, privacy, and internal audit teams. Customers using Google Cloud Platform retain all rights and respons bilities to configure and manage their environment.
T36	Google is certified to the ISO27001 Standard, which regulates "Access Control" (ISO 27001:2013, Annex A.9). Information security oversight and management controls, including logical access controls are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. For Google employees, access rights and levels are based on an their job function and role, using the concepts of least–privilege and need–to–know to match access privileges to defined respons bilities. Google employees are only granted a limited set of default permissions to access company resources, such as employee email and Google's internal employee portal. Requests for additional access follow a formal process that involves a request and an approval from a data or system owner, manager, or other executives, as dictated by Google's security policies. Approvals are managed by workflow tools that maintain audit records of all changes. These tools control both the modification of authorization settings and the approval process to ensure consistent application of the approval policies. An employee's authorization settings are used to control access to all resources, including data and systems for Google Cloud and G Suite products. Support services are only provided to authorized customer administrators whose identities have been verified in several ways. Googler access is monitored and audited by our dedicated security, privacy, and internal audit teams. Customers using Google Cloud Platform retain all rights and respons bilities to configure and manage their environment.
T37	Google is certified to the ISO27001 Standard, which regulates "Access Control" (ISO 27001:2013, Annex A.9). Information security oversight and management controls, including logical access controls are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. For Google employees, access rights and levels are based on an their job function and role, using the concepts of least–privilege and need–to–know to match access privileges to defined respons bilities. Google employees are only granted a limited set of default permissions to access company resources, such as employee email and Google's internal employee portal. Requests for additional access follow a formal process that involves a request and an approval from a data or system owner, manager, or other executives, as dictated by Google's security policies. Approvals are managed by workflow tools that maintain audit records of all changes. These tools control both the modification of authorization settings and the approval process to ensure consistent application of the approval policies. An employee's authorization settings are used to control access to all resources, including data and systems for Google Cloud and G Suite products. Support services are only provided to authorized customer administrators whose identities have been verified in several ways. Googler access is monitored and audited by our dedicated security, privacy, and internal audit teams. Customers using Google Cloud Platform retain all rights and respons bilities to configure and manage their environment.
T38	Responsibility for the prevention of unauthorized use resides with the customer.
T39	Responsibility for the prevention of unauthorized use resides with the customer.
T40	Customers are required to take appropriate precautions to prevent the use of counterfeit cards.
T41	Customers are required to take appropriate precautions to prevent the use of counterfeit cards.
T42	Google is certified to the ISO27001 Standard, which regulates "Cryptography" (ISO 27001:2013, Annex A.10) Google publishes details about encryption and key management options for its Google Cloud and G Suite products. To read more about key management and encryption, please see: https://cloud.google.com/security/encryption-at-rest/ https://storage.googleapis.com/gfw-touched-accounts-pdfs/google-encryption-whitepaper-G Suite.pdf Customers using Google Cloud Platform retain all rights and respons bilities to configure and manage their environment, including development of appropriate encryption measures.
T42-1	Customers are required to take appropriate precautions to prevent unauthorized browsing.
T43	Google is certified to the ISO27001 Standard, which regulates "Access to Networks and Network Services" (ISO27001:2013, Annex A.9.1.2), "Network Security Management" (ISO27001:2013, Annex A.13.1). We have a rigorous incident management process for security events that may affect the confidentiality, integrity, or availability of systems or data. If an incident occurs, the security team logs and prioritizes it according to its severity. Events that directly impact customers are assigned the highest priority. This process specifies courses of action, procedures for notification, escalation, mitigation, and documentation. Google's security incident management program is structured around the NIST guidance on handling incidents (NIST SP 800–61). Key staff are trained in forensics and handling evidence in preparation for an event, including the use of third-party and proprietary tools. Testing of incident response plans is performed for key areas, such as systems that store sensitive customer information. These tests take into consideration a variety of scenarios, including insider threats and software vulnerabilities. To help ensure the swift resolution of security incidents, the Google security team is available 24/7 to all employees. If an incident involves customer data, Google or its partners will inform the customer and support investigative efforts via our support team. Customers using Google Cloud Platform retain all rights and respons bilities to configure and manage their environment and ensure unauthorized access is detected and reviewed appropriately.
T44	Google is certified to the ISO27001 Standard, which regulates "Access to Networks and Network Services" (ISO27001:2013, Annex A.9.1.2), "Network Security Management" (ISO27001:2013, Annex A.13.1). We have a rigorous incident management process for security events that may affect the confidentiality, integrity, or availability of systems or data. If an incident occurs, the security team logs and prioritizes it according to its severity. Events that directly impact customers are assigned the highest priority. This process specifies courses of action, procedures for notification, escalation, mitigation, and documentation. Google's security incident management program is structured around the NIST guidance on handling incidents (NIST SP 800–61). Key staff are trained in forensics and handling evidence in preparation for an event, including the use of third-party and proprietary tools. Testing of incident response plans is performed for key areas, such as systems that store sensitive customer information. These tests take into consideration a variety of scenarios, including insider threats and software vulnerabilities. To help ensure the swift resolution of security incidents, the Google security team is available 24/7 to all employees. If an incident involves customer data, Google or its partners will inform the customer and support investigative efforts via our support team. Customers using Google Cloud Platform retain all rights and respons bilities to configure and manage their environment and ensure unauthorized access is detected and reviewed appropriately.
T45	Google is certified to the ISO27001 Standard, which regulates "Access to Networks and Network Services" (ISO27001:2013, Annex A.9.1.2), "Network Controls" (ISO27001:2013, Annex A.13.1.1). We have a rigorous incident management process for security events that may affect the confidentiality, integrity, or availability of systems or data. If an incident occurs, the security team logs and prioritizes it according to its severity. Events that directly impact customers are assigned the highest priority. This process specifies courses of action, procedures for notification, escalation, mitigation, and documentation. Google's security incident management program is structured around the NIST guidance on handling incidents (NIST SP 800–61). Key staff are trained in forensics and handling evidence in preparation for an event, including the use of third-party and proprietary tools. Testing of incident response plans is performed for key areas, such as systems that store sensitive customer information. These tests take into consideration a variety of scenarios, including insider threats and software vulnerabilities. To help ensure the swift resolution of security incidents, the Google security team is available 24/7 to all employees. If an incident involves customer data, Google or its partners will inform the customer and support investigative efforts via our support team. Customers using Google Cloud Platform retain all rights and respons bilities to configure and manage their environment and ensure unauthorized access is detected and reviewed appropriately.

T46	Customers are required to configure parameters to identify transactional anomalies.
T47	Customers are required to configure parameters to identify transactional anomalies.
T48	Google is certified to the ISO27001 Standard, which regulates "Access to Networks and Network Services" (ISO27001:2013, Annex A.9.1.2), "Network Controls" (ISO27001:2013, Annex A.13.1.1). We have a rigorous incident management process for security events that may affect the confidentiality, integrity, or availability of systems or data. If an incident occurs, the security team logs and prioritizes it according to its severity. Events that directly impact customers are assigned the highest priority. This process specifies courses of action, procedures for notification, escalation, mitigation, and documentation. Google's security incident management program is structured around the NIST guidance on handling incidents (NIST SP 800–61). Key staff are trained in forensics and handling evidence in preparation for an event, including the use of third-party and proprietary tools. Testing of incident response plans is performed for key areas, such as systems that store sensitive customer information. These tests take into consideration a variety of scenarios, including insider threats and software vulnerabilities. To help ensure the swift resolution of security incidents, the Google security team is available 24/7 to all employees. If an incident involves customer data, Google or its partners will inform the customer and support investigative efforts via our support team. Customers using Google Cloud Platform retain all rights and respons bilities to configure and manage their environment and ensure unauthorized access is detected and reviewed appropriately.
T49	Google is certified to the ISO27001 Standard, which regulates "Protection from Malware" (Annex A.12.2). Controls relating to vulnerability management are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google administers a vulnerability management process that actively scans for security threats using a combination of commercially available and purpose-built in house tools, intensive automated and manual penetration efforts, quality assurance processes, software security reviews and external audits. The vulnerability management team is respons ble for tracking and following up on vulnerabilities. Once a vulnerability requiring remediation has been identified, it is logged, prioritized according to severity, and assigned an owner. The vulnerability management team tracks such issues and follows up frequently until they can verify that the issues have been remediated. Google also maintains relationships and interfaces with members of the security research community to track reported issues in Google services and open source tools. More information about reporting security issues can be found at www.google.com/intl/en/corporate/security.html.
T50	Google is certified to the ISO27001 Standard, which regulates "Protection from Malware" (Annex A.12.2). Controls relating to vulnerability management are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google administers a vulnerability management process that actively scans for security threats using a combination of commercially available and purpose-built in house tools, intensive automated and manual penetration efforts, quality assurance processes, software security reviews and external audits. The vulnerability management team is respons ble for tracking and following up on vulnerabilities. Once a vulnerability requiring remediation has been identified, it is logged, prioritized according to severity, and assigned an owner. The vulnerability management team tracks such issues and follows up frequently until they can verify that the issues have been remediated. Google also maintains relationships and interfaces with members of the security research community to track reported issues in Google services and open source tools. More information about reporting security issues can be found at www.google.com/intl/en/corporate/security.html.
T51	Google is certified to the ISO27001 Standard, which regulates "Protection from Malware" (Annex A.12.2). Controls relating to vulnerability management are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google administers a vulnerability management process that actively scans for security threats using a combination of commercially available and purpose-built in house tools, intensive automated and manual penetration efforts, quality assurance processes, software security reviews and external audits. The vulnerability management team is respons ble for tracking and following up on vulnerabilities. Once a vulnerability requiring remediation has been identified, it is logged, prioritized according to severity, and assigned an owner. The vulnerability management team tracks such issues and follows up frequently until they can verify that the issues have been remediated. Google also maintains relationships and interfaces with members of the security research community to track reported issues in Google services and open source tools. More information about reporting security issues can be found at www.google.com/intl/en/corporate/security.html.